Holland & Knight

1650 Market Street, Suite 3300 | Philadelphia, PA 19103 | T 215.252.9600 | F 215.867.6070
Holland & Knight LLP | www.hklaw.com

Richard Harris
215.252.9594
Richard.Harris@hklaw.com

Paul Bond
215.252.9535
Paul.Bond@hklaw.com

March 26, 2025

VIA ECF

Honorable John M. Younge
United States District Court
Eastern District of Pennsylvania
15613 U.S. Courthouse
601 Market Street, Courtroom 15-B
Philadelphia, PA 19106

RE: Kenneth Hasson v. Comcast Cable Communications, LLC, et al.
Case No.: 2:23-cv-05039-JMY

Dear Judge Younge:

Defendants Comcast Communications Corporation, LLC and Comcast Corporation ("Comcast") write with a supplement to their letter of March 24, 2025. **[DE #174]**. In that letter, Comcast informed the Court that Lead Interim Class Counsel in *Hasson* had filed a copycat lawsuit in California state court without notice or explanation to this Court or Defendants' counsel.[1] As a result, and at Comcast's request, the Court Ordered a hearing by video to take place on April 1, 2025, at 2 p.m. **[DE #75]**. In light of the events set forth below, Comcast respectfully requests that the hearing take place in person before Your Honor.

Lead Interim Class Counsel in *Hasson* has now filed yet ***another*** nearly-identical putative class action against Comcast and its co-defendants Citrix Systems, Inc. and Cloud Software Group, Inc.—this time in Pennsylvania state court. Please see attached, the Complaint in *Ryan Emmett v. Comcast Cable Communications, LLC*, *Comcast Corporation, Citrix Systems, Inc., and Cloud Software Group, Inc.* (hereafter, "*Emmett*"), filed in the Court of Common Pleas for Allegheny County (No. GD-25-003268).

[1] Namely, *Margaret Scheirer v. Comcast Communications Corporation, LLC, Comcast Corporation, Citrix Systems, Inc., and Cloud Software Group, Inc*. (hereafter, "*Scheirer*"), filed in the Superior Court for the State of California, County of Alameda (no docket number yet assigned).

Emmett targets the same defendants as *Hasson* and *Scheirer*, arises from the exact same 2023 attack on Comcast, and makes the same Cable Act claims and other claims previously made in *Hasson* and *Scheirer*. *Hasson* and *Scheirer* both propose nationwide classes, *Emmett* proposes a 49-state class (excluding only California). Lead Interim Class Counsel are filing essentially the same case over and over, in different fora before different judges.

Meanwhile, as Lead Interim Class Counsel are "weighing their options" about whether to proceed in state or federal court, Plaintiffs are wasting Defendants' and the Court's time and resources with jurisdictional discovery that Plaintiffs demanded in *Hasson*. Indeed, ***three*** jurisdiction-related depositions have been taken since March 24, 2025, the day Lead Interim Class Counsel filed *Scheirer***.**

Comcast looks forward to discussing these issues with the Court on Tuesday. Comcast respectfully requests, however, that the hearing be held in person in Philadelphia given the importance of the issues. Comcast requests that the hearing proceed even if Lead Interim Class Counsel attempts to dismiss *Hasson* before then, as the record may be useful to any subsequent court considering Lead Interim Class Counsel's adequacy to represent a class under Rule 23 or its state court equivalent.

Respectfully submitted,

Richard Harris
Paul Bond

EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Allegheny County

For Prothonotary Use Only:	TIME STAMP
Docket No:	

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
Ryan Emmett	Comcast Cable Communications, LLC
Are money damages requested? ☐ Yes ☒ No	Dollar Amount Requested: (check one) ☐ within arbitration limits ☒ outside arbitration limits
Is this a *Class Action Suit*? ☒ Yes ☐ No	**Is this an *MDJ Appeal*?** ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: Gary F. Lynch

☐ **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE.*** If you are making more than one type of claim, check the one that you consider most important.

TORT (*do not include Mass Tort*)
- ☐ Intentional
- ☐ Malicious Prosecution
- ☐ Motor Vehicle
- ☐ Nuisance
- ☐ Premises Liability
- ☐ Product Liability *(does not include mass tort)*
- ☐ Slander/Libel/ Defamation
- ☐ Other:

MASS TORT
- ☐ Asbestos
- ☐ Tobacco
- ☐ Toxic Tort - DES
- ☐ Toxic Tort - Implant
- ☐ Toxic Waste
- ☐ Other:

PROFESSIONAL LIABLITY
- ☐ Dental
- ☐ Legal
- ☐ Medical
- ☐ Other Professional:

CONTRACT (*do not include Judgments*)
- ☐ Buyer Plaintiff
- ☐ Debt Collection: Credit Card
- ☐ Debt Collection: Other
- ☐ Employment Dispute: Discrimination
- ☐ Employment Dispute: Other
- ☒ Other: Data breach

REAL PROPERTY
- ☐ Ejectment
- ☐ Eminent Domain/Condemnation
- ☐ Ground Rent
- ☐ Landlord/Tenant Dispute
- ☐ Mortgage Foreclosure: Residential
- ☐ Mortgage Foreclosure: Commercial
- ☐ Partition
- ☐ Quiet Title
- ☐ Other:

CIVIL APPEALS
Administrative Agencies
- ☐ Board of Assessment
- ☐ Board of Elections
- ☐ Dept. of Transportation
- ☐ Statutory Appeal: Other
- ☐ Zoning Board
- ☐ Other:

MISCELLANEOUS
- ☐ Common Law/Statutory Arbitration
- ☐ Declaratory Judgment
- ☐ Mandamus
- ☐ Non-Domestic Relations Restraining Order
- ☐ Quo Warranto
- ☐ Replevin
- ☐ Other:

NOTICE

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides, in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

(i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.

(ii) actions for support, Rules 1910.1 et seq.

(iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.

(iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.

(v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.

(vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (e) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

RYAN EMMETT, on behalf of himself and all others similarly situated,

Plaintiff,

v.

COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, CITRIX SYSTEMS, INC., and CLOUD SOFTWARE GROUP, INC,

Defendants.

CIVIL DIVISION – CLASS ACTION

No.

CLASS ACTION COMPLAINT

Filed on behalf of Plaintiff, RYAN EMMETT

Counsel of Record for this Party:

GARY F. LYNCH
PA ID No. 56887
CONNOR P. HAYES
PA ID No. 330447

LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: 412-322-9243
gary@lcllp.com
connorh@lcllp.com

[Additional counsel in signature block]

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

RYAN EMMETT, on behalf of himself and all others similarly situated,

Plaintiff,

v.

COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, CITRIX SYSTEMS, INC., and CLOUD SOFTWARE GROUP, INC.,

Defendants.

CIVIL DIVISION – CLASS ACTION

No.

NOTICE TO DEFEND

YOU HAVE BEEN SUED IN COURT. If you wish to defend against the claims set forth in the following pages, you must take action within **TWENTY (20)** days after this Complaint and Notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the Complaint or for any claim or relief requested by the Plaintiff. You may lose money or property or other rights important to you. **YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE.**

IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.

IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

LAWYER REFERRAL SERVICE
The Allegheny County Bar Association
11th Floor Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: (412) 261-5555

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

RYAN EMMETT, on behalf of himself and all others similarly situated,

Plaintiff,

v.

COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, CITRIX SYSTEMS, INC., and CLOUD SOFTWARE GROUP, INC.,

Defendants.

CIVIL DIVISION – CLASS ACTION

No.

CLASS ACTION COMPLAINT

Plaintiff Ryan Emmett, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Comcast Corporation and Comcast Cable Communications, LLC (collectively, "Comcast"), and Citrix Systems, Inc. and Cloud Software Group, Inc. (collectively, "Citrix," and together with Comcast, "Defendants"), seeking monetary damages, restitution, and injunctive relief arising from a data breach that resulted in the theft of Plaintiff's highly sensitive personal information. Plaintiff makes the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation of counsel, a review of public documents, and other facts that are a matter of public record.

NATURE OF THE ACTION

1. Comcast is one of the largest companies in the telecommunications sector and provides internet services and products, cable television, a mobile 5G network, and landline telephone services and products to individuals and businesses across the United States under the brand name Xfinity. To obtain any of these Xfinity services, customers are required to entrust

Comcast with their PII, which Comcast uses to engage in its usual business activities. Comcast understands that it has an enormous responsibility to protect the data it collected, assuring its customers that "Your Data Privacy is Our Top Priority."[1] Despite this assurance to its customers, however, Comcast failed to protect the very customer information it was entrusted, leading to a data breach of Comcast's systems that stemmed from a vulnerability in Citrix's software and appliances that Comcast utilized and failed to timely patch, compromising the personal information of approximately 36 million people.

2. Citrix is one of the largest companies in the office technology sector and provides an array of business technology services, including server, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing services to hundreds of thousands of clients worldwide. Comcast contracted with Citrix to provide a variety of networking hardware and software services, including the use of Citrix NetScaler ADC and NetScaler Gateway (the "NetScaler products").

3. Together, Defendants Comcast and Citrix failed to properly secure and safeguard the highly valuable, personally identifiable information of approximately 36 million Comcast customers, including customers' usernames and hashed passwords, names, contact information, full and partial Social Security numbers, driver's license numbers, dates of birth, secret security questions and answers, and other personal data (collectively, "PII"). Comcast failed to comply with industry standards to protect Plaintiff's and Class Members' PII in its computer systems. And because of the inadequacy of Comcast's post-Data Breach investigation, Comcast failed to provide

[1] *2022 Xfinity Cyber Health Report*, Comcast (2022), https://update.comcast.com/wp-content/uploads/sites/33/dlm_uploads/2022/12/2022-Xfinity-Cyber-Health-Report-12.13.22-5pm-reduced.pdf at 17.

adequate notice to Plaintiff and other members of the Class that their PII had been accessed and acquired.

4. Defendants are well-aware of the foreseeable risks of implementing inadequate data security measures, as some of the largest data breaches of the past year have resulted from vulnerabilities in third-party products, including the MOVEit Transfer and GoAnyWhere MFT data breaches. They also expressly recognize such risks in their SEC filings as a threat to their businesses. Despite this foreseeability, Defendants failed to implement adequate data security measures. On October 10, 2023, Citrix publicly announced that it had discovered multiple critical vulnerabilities in its Citrix NetScaler products, which became widely known among cybersecurity commentators as the "Citrix Bleed" vulnerability. As part of the announcement, Citrix released a security patch that customers could implement to eliminate the Citrix Bleed vulnerability and to prevent unauthorized access to customers' systems that contain PII.

5. Comcast failed to timely install the security patch in its Citrix NetScaler products, and, as a result, between October 16 and October 19, 2023, cybercriminals exploited the vulnerabilities, accessed Comcast's internal systems, and accessed and acquired the PII of approximately 36 million Xfinity customers (the "Data Breach" or "Breach" herein).

6. Although the vulnerability was exploited because Comcast failed to timely patch its systems, if Comcast had industry standard cybersecurity measures already in place, such as the deletion of former customers' PII, employing the data security principle of least privilege (PoLP), and using proper session management protocols, the PII of 36 million customers would not have been acquired by cybercriminals.

7. Defendant Citrix is equally blameworthy. Citrix failed to adequately monitor, test, and secure its appliances that it provided to Comcast, although it knew or should have known that

Comcast would use such appliances to remotely access its internal networks where Comcast stores Plaintiff's and Class members' PII. In addition, Citrix failed to provide complete patching guidance to Comcast despite publicizing the vulnerability to the world, including cybercriminals. Citrix also downplayed the severity of the vulnerability to Comcast to avoid fracturing its business relationship. It was not until two weeks after its initial announcement that Citrix revealed the true magnitude of the vulnerability and provided sufficient guidance for its customers to fully patch their vulnerable appliances. But by then, the damage was done.

8. As a direct and proximate result of Comcast's failure to follow industry-standard practices to secure and protect the information, timely implement the security patch and follow basic security procedures, and as a direct and proximate result of Citrix's failure to adequately secure, test, and monitor its widely-used network products before selling those products to customers like Comcast who foreseeably used those products to handle sensitive PII, and, as a direct and proximate result of Citrix's failure to timely disclose vulnerabilities in its products and to provide complete patching guidance with reasonable care, Plaintiff's and Class Members' PII is now in the hands of cybercriminals.

9. As a result of Defendants' conduct, Plaintiff and Class Members now face an imminent and substantial risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Comcast's and Citrix's unlawful and tortiously deficient data security practices have injured millions of consumers, and Plaintiff and putative Class Members in this action therefore bring claims for negligence, negligence *per se*, breach of express and implied contract,

unjust enrichment, and an array of state and federal statutory claims, seeking damages, declaratory relief, and injunctive relief.

PARTIES

11. Plaintiff Ryan Emmett is an adult individual and a natural person of the Commonwealth of Pennsylvania, residing in Allegheny County, where he intends to stay, and therefore is a citizen of the Commonwealth of Pennsylvania. Plaintiff has been a Comcast customer since 2023. On information and belief, Plaintiff's name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and/or Comcast security questions and answers were potentially compromised in the Data Breach.

12. Plaintiff only allowed Comcast and its vendors, including Citrix, to maintain, store, and use his PII because he reasonably expected that Defendants would use basic security measures to protect his PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing his PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff entrusted his PII to Comcast and its vendors, and his PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff been informed of Comcast's and Citrix's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Defendants.

13. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

14. As a result of the Data Breach, Plaintiff has been further injured by the damages to and loss in value of his PII—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

15. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his PII. This highly sensitive information, which includes his name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

16. Upon information and belief, Plaintiff's PII has already been stolen and misused.

17. As a result of the harm Plaintiff has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

18. Comcast acknowledged the risk posed to Plaintiff and his PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[2]

19. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as

[2] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited Mar. 20, 2025).

soon as possible," as "exploits of [the Citrix Bleed vulnerability] on unmitigated appliances have been observed."[3]

20. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

21. Defendant Comcast Corporation is a Pennsylvania corporation with its principal place of business located at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103.

22. Defendant Comcast Cable Communications, LLC is a Delaware limited liability company that maintains its headquarters at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103. Upon information and belief, Comcast Corporation is the only member of Comcast Cable Communications, LLC. Defendant Comcast Cable Communications, LLC is a citizen of each state in which its members are citizens. As such, Defendant Comcast Cable Communications, LLC is a citizen of Pennsylvania.

23. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida, and is therefore a citizen of Florida. Citrix's direct parent corporation is Picard Parent, Inc. Picard Parent, Inc. is a direct, wholly owned subsidiary of Cloud Software Group, Inc., which is a direct wholly owned subsidiary of Cloud Software Holdings, Inc., which is a direct, wholly owned subsidiary of Picard Holdco, Inc.

24. Defendant Cloud Software Group, Inc. is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida and is therefore a citizen of Florida. Cloud Software

[3] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix, https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 (last modified Nov. 27, 2023) (hereinafter "Citrix Bleed Security Bulletin").

Group, Inc. is a direct, wholly owned subsidiary of Cloud Software Holdings, Inc., which is a direct, wholly owned subsidiary of Picard Holdco, Inc.

JURISDICTION AND VENUE

25. The Court has subject matter jurisdiction over this action pursuant to Pa. Cons. Art. 5 § 5 and 42 Pa. C.S.A. § 931(b).[4]

26. The Court has personal jurisdiction over Defendants pursuant to 42 Pa. C.S.A. §§ 5301(a)(2) and 5308.

27. Venue is proper in this County pursuant to Pa. R. Civ. P. 2179(a) because it is where Defendants regularly conduct business in this county, and the cause of action arose in this county.

FACTUAL BACKGROUND

A. Comcast Obtains, Collects, and Stores Plaintiff's and Class Members' Private, Personally Identifiable Information.

28. Comcast is one of the largest companies in the American telecommunications sector, and provides internet services and products, cable television, mobile 5G network cellular services, and landline telephone services and products to individuals and businesses across the United States under the brand name Xfinity.[5]

29. The bulk of Comcast's consumer-facing business comes from its cable communications services, which include broadband, video, voice, wireless, and other services that are offered individually and as bundled services to residential customers nationwide. According to its 2022 Annual Report, Comcast provides its cable communications services to almost 32 million

[4] In other litigation, Defendants have argued that there is no federal Article III standing for claims like Plaintiff's arising from the Data Breach, so Plaintiff's claims are properly before this Court instead of federal court.

[5] *Comcast 2022 Annual Report on Form 10-K*, https://www.cmcsa.com/static-files/156da323-653e-4cc6-9bb4-d239937e9d2f (last visited Mar. 20, 2025).

residential customers.[6] While Comcast, under the Xfinity brand, primarily serves residential customers, Comcast also boasts a sprawling business division that serves over 2 million business services customers, with Xfinity's business operations recently "approaching $10 billion in annual revenue."[7]

30. Xfinity's reach is substantial, even compared to its competitors across the United States, with Comcast claiming that Xfinity is now the "largest internet provider in the U.S."[8] In many of the markets where it operates, Xfinity is the only provider of these services to consumers.[9]

31. Beyond traditional cable communications services, Xfinity also operates a nationwide network of 20 million internet hot spots, which non-residential services customers can sign up to utilize under an array of hotspot-only internet plans.[10]

32. Comcast also offers 5G network wireless cellular service plans under the Xfinity Mobile and NOW Mobile brands that leverage the extensive Xfinity internet hot spot network. These services are also fast-growing, with more than six million customers.[11]

33. To run its business, Comcast collects, maintains, and profits from the PII of millions of U.S. consumers. Depending on the Xfinity product(s) that customers sign up for, Comcast requires customers to provide their name, phone number, residential address, date of birth, last four digits of their Social Security number, driver's license number, demographic information,

---

[6] *Id*.
[7] *Connectivity & Platforms*, Comcast, https://corporate.comcast.com/company/connectivity-platforms (last visited Mar. 20, 2025).
[8] *Id*.
[9] Karl Bode, *The Future of American Broadband is a Comcast Monopoly*, Vice (Dec. 18, 2018), https://www.vice.com/en/article/the-future-of-american-broadband-is-a-comcast-monopoly/.
[10] *Xfinity Wifi*, Xfinity, https://www.xfinity.com/learn/internet-service/wifi (last visited Mar. 20, 2025).
[11] *Wireless*, Comcast, https://corporate.comcast.com/company/xfinity/wireless (last visited Mar. 20, 2025).

their mobile phone's unique technical identifier (also known as an International Mobile Equipment Identity or "IMEI" number), information and forms required for proof of residency, credit card or debit card information, and/or bank account information. Comcast collects this PII from all prospective and current customers and maintains and profits from the PII regardless of whether a potential customer eventually purchases Xfinity services. Comcast also maintains the PII of former Xfinity customers for an indefinite period after they terminate their Xfinity services.

34. To use any of Comcast's Xfinity services, customers must also create an online account with Xfinity and create a username, password, and secret questions and answers to assist with account recovery.

B. Comcast Knows the Risk of Storing PII and Promises to Keep Customers' PII Secure.

35. As a company storing and using sensitive customer data, Comcast is at great risk of cyberattacks. Comcast is well-aware of this risk and expressly represents to customers that it will protect their PII.

36. Comcast recognizes the foreseeable risk of cyberattacks it faces. In Comcast's 2022 Cyber Health Report, Comcast states "[w]e know that our customers' data is what bad actors are after" and states "[d]ata breaches have become a part of daily life. We hear about a breach on the news and we hope we don't get the dreaded email saying our data was compromised. But while data breaches may seem sadly normal, we don't think they have to be, and we're committed to helping prevent them."[12]

37. Comcast's 2022 Cyber Health Report similarly recognizes that it is Comcast's responsibility to safeguard its customers' PII, not the other way around: "[w]e don't expect our

[12] 2022 Cyber Health Report, *supra* note 1, at 1, 12.

customers to be cybersecurity experts. That's why we make a point of prioritizing security for them, from the gateway in their home through to the core of our network."[13]

38. Further, Comcast has an entire sub-page of the Xfinity website dedicated to customer data protection and privacy. At the top of this Privacy sub-page, Comcast represents to consumers that "[y]our privacy matters to us," and emphasizes that "[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it."[14]

39. Indeed, Comcast explicitly states "[w]e believe strong cybersecurity is essential to privacy," and highlights to customers that it works tirelessly to protect their sensitive information from cyberattacks:

> We help protect you with multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second and a team of security experts who work to protect you 24 hours a day, 365 days a year.[15]

40. Comcast goes on to describe all the "tools and support" it provides to help customers "stay safe online," including "free security software and tools, like multi-factor authentication," and "access to free online tips and advice and an Xfinity security and privacy team to help protect you and your family from cyber threats."[16]

41. The Xfinity Privacy Policy similarly goes to great lengths to promise customers that Comcast will protect the PII that it collects:

> We follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices include

[13] *Id.* at 1.
[14] *Privacy*, Xfinity, http://xfinity.com/privacy (last visited Mar. 20, 2025).
[15] *Id.*
[16] *Id.*

> technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information. Although we take the responsibility of safeguarding your personal information seriously, no security measures are 100% effective and we cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose your information. Comcast also takes additional steps to increase the security and reliability of customer communications. We do not read your outgoing or incoming email, file attachments, video mail, private chat, or instant messages. However, we (along with our service providers) use software and hardware tools to help prevent and block "spam" emails, viruses, spyware, and other harmful or unwanted communications and programs from being sent and received over Comcast.net email and the Comcast Services. To help protect you and the Services against these harmful or unwanted communications and programs, these tools may automatically scan your emails, video mails, instant messages, file attachments, and other files and communications. We do not use these tools for marketing or advertising.[17]

42. Comcast also acknowledged the risk of inadequate data security—including through use of third-party products and services—in its SEC filings:

> … In the ordinary course of our business, there are constant attempts by third parties to cause systems-related events and security incidents and to identify and exploit vulnerabilities in security architecture and system design. These incidents include computer hackings, cyber attacks, computer viruses, worms or other destructive or disruptive software, denial of service attacks, phishing attacks, malicious social engineering, and other malicious activities. Incidents also may be caused inadvertently by us or our third-party vendors, such as process breakdowns and vulnerabilities in security architecture or system design. . . . Moreover, as we also obtain certain confidential, proprietary and personal information about our customers, personnel and vendors, and in some cases provide this information to third party vendors who agree to protect it, we face the risk that this information may become compromised through a cyber attack or data breach, misappropriation, misuse, leakage, falsification or accidental release or loss of information. Due to the nature of our businesses, we may be at a disproportionately heightened risk of these types of incidents occurring because we maintain certain information necessary to conduct our business in digital form. We also incorporate third-party software (including extensive open-source software), applications, and data hosting and cloud-based services into many aspects of our products, services and operations, as well as rely on service providers to help us perform our business

[17] *Our Privacy Policy*, Xfinity https://web.archive.org/web/20231128085904/https://assets.xfinity.com/assets/dotcom/projects/cix-5055_xfinity-com-welcome-kit-legal/PP_09202023.pdf (last visited Mar. 20, 2025).

> operations, all of which expose us to cyber attacks on such third-party suppliers and service providers.
>
> While we develop and maintain systems, and operate extensive programs that seek to prevent security incidents from occurring, these efforts are costly and must be constantly monitored and updated in the face of sophisticated and rapidly evolving attempts to overcome our security measures and protections. . . . Despite our efforts, we expect that we will continue to experience such incidents in the future, and there can be no assurance that any such incident will not have an adverse effect on our business, reputation or results of operations.[18]

43. The risk that cybercriminals will breach Comcast's systems and gain unauthorized access to customers' PII, and use that information for malicious purposes, is not theoretical. As Comcast itself states, Comcast is bombarded with "hundreds of thousands of cyber events every second."[19]

44. In fact, Comcast's systems have previously been breached at least three times, which should have put Comcast on notice as to both weaknesses in its security practices as well as cybercriminals' desire to target its systems.

45. In 2015, for example, a hacker breached Comcast's systems and stole nearly 590,000 then-current and former Comcast email addresses and passwords, which the hacker subsequently posted for sale on the "dark web."[20] The dark web is a heavily encrypted part of the Internet that conceals users' identities and online activity, and makes it difficult for authorities to detect the location or owners of a website when illegally-acquired information is disclosed or put up for sale.

---

[18] *Comcast 2022 Annual Report on Form 10-K*, Comcast (Feb. 3, 2023), https://www.cmcsa.com/static-files/b5959ccc-6216-4bbb-a0ca-de6f689925f7.
[19] Xfinity Privacy Center, https://www.xfinity.com/privacy (last visited Mar. 24, 2025).
[20] Pierluigi Paganini, *200,000 Comcast Login Credentials Available on the Dark Web*, Security Affairs (Nov. 10, 2015), https://securityaffairs.com/41875/cyber-crime/200000-comcast-login-darkweb.html.

46. In 2021, hackers were able to breach Comcast's systems and display a cryptic message to any Xfinity customer that logged into their account. Starting on December 19th, many Xfinity email users began receiving notifications that their account information had been changed. However, when attempting to access the accounts, they could not log in as the passwords had been changed. "After regaining access to the accounts, they discovered they had been hacked and a secondary email at the disposable @yopmail.com domain was added to their profile."[21]

47. And in 2022, Comcast was the victim of yet *another* breach, when cybercriminals were able to bypass Xfinity's two-factor authentication safeguard and compromise an unidentified number of Xfinity accounts.[22]

48. At all relevant times, Comcast therefore knew of the attendant risks that it and its customers faced as a result of collecting and storing the PII of millions of individuals and was well-aware that it must develop a robust cybersecurity program, including developing policies to prevent additional data breaches moving forward.

49. Indeed, because of the highly sensitive and personal nature of Plaintiff's PII that Comcast collects and stores, Comcast has publicly affirmed its obligation and duty to secure PII, as noted *supra*.

50. Despite Comcast's duty, and its representations made to its consumers, Comcast's data security practices fell flat, leading to the Data Breach and the compromise of its customers' PII.

[21] Sarah J. Callahan, *Comcast Customers Face a Huge Holiday Data Breach*, The Street (Dec. 24, 2022), https://www.thestreet.com/technology/comcast-xfinity-data-breach-two-factor-auth-help-bypass.
[22] *Id.*

C. Comcast Engaged Citrix to Provide Secure Remote Access to Comcast's Internal Network, which Stores Plaintiff's and Class Members' PII.

51. As part of its strategy to protect and safeguard the PII that customers had entrusted to it, Comcast contracted with Defendant Citrix to implement the NetScaler Products to provide secure remote access for Comcast employees to access Comcast's internal networks.

52. Founded in 1989, Citrix Systems has grown into one of the largest companies in the office technology sector. It provides an array of cloud computing and virtualization products to hundreds of thousands of clients worldwide, including server, application and desktop virtualization, networking, software as a service (SaaS), and other cloud-related services. As of 2024, Citrix cloud-related services alone are used by over 16 million customers.[23]

53. In 2016, Citrix Systems consolidated all of its networking products under the NetScaler product line. The NetScaler line includes NetScaler ADC, an application delivery controller (ADC), NetScaler AppFirewall, an application firewall, NetScaler Unified Gateway, which offered remote access to virtual desktops, NetScaler Application Delivery Management (ADM), and NetScaler SD-WAN, which provides software-defined wide-area networking management.

54. The NetScaler products at issue here combine to purportedly improve the efficiency and speeds of applications (NetScaler ADC) and consolidate remote access infrastructure by providing a single-sign-on across all applications (NetScaler Gateway).[24]

55. One of the primary functionalities provided by Citrix NetScaler products is ensuring secure access to Virtual Desktop Infrastructure, a network service that allows remote

[23] *About*, Citrix, https://www.citrix.com/about/ (last visited Mar. 20, 2025).
[24] *See What is an application delivery controller?*, Citrix, https://www.netscaler.com/articles/what-is-an-application-delivery-controller (last visited Mar. 20, 2025); *NetScaler Gateway*, NetScaler (Jan. 8, 2024), https://docs.netscaler.com/en-us/netscaler-gateway.html.

users such as employees working from home to access a (virtual) desktop computer located within the private network of a business organization such as Comcast.[25] When a user logs into such a virtual desktop, the user's actual device can view a live image of the remote computer's desktop (or a specific application window on the remote desktop, such as a Microsoft Excel window) and the user can use their mouse and keyboard to interact with the remote desktop using an application or their web browser.

56. NetScaler was spun off into a different business unit of Cloud Software Group, Inc., Citrix Systems' parent company, when Citrix Systems was taken private in 2022. Citrix is responsible for maintenance and support of the NetScaler line of products as recently as the Data Breach, as Citrix released the patch for the NetScaler vulnerability that was exploited in the Data Breach.[26]

57. NetScaler products are widely used across a variety of industries, with an estimated seventy-five percent of all Internet traffic passing through NetScaler Products every day.[27] As a result, NetScaler products are frequent targets for cybercriminals, particularly given that NetScaler products can grant highly privileged access to targeted networks.[28]

58. Citrix knows that its products are used to manage highly sensitive information and the risks that come from storing and managing sensitive customer information.

---

[25] *Setting up NetScaler for Citrix Virtual Apps and Desktops*, Citrix, https://docs.netscaler.com/en-us/citrix-adc/current-release/solutions/deploy-xa-xd.html.
[26] Citrix Bleed Security Bulletin, *supra* note 3.
[27] Val King, *Citrix ADC, NetScaler Gateway, and NetScaler ADCs*, WhiteHat (Dec. 3, 2021), https://blog.whitehatvirtual.com/what-does-a-citrix-netscaler-actually-do.
[28] Jai Vijayan, *Unpatched Citrix NetScaler Devices Targeted by Ransomware Group FIN8*, Dark Reading (Aug. 29, 2023), https://www.darkreading.com/cyberattacks-data-breaches/unpatched-citrix-devices-targeted-by-ransomware-group-fin8.

59. Furthermore, Citrix recognizes that "[a]ctual or perceived security vulnerabilities in our products and services or cyberattacks on our services infrastructure or corporate networks" as a risk to its business in Citrix's 10-K Annual Report.[29] And Citrix explains why these vulnerabilities and cyberattacks on its infrastructure are a risk to its business:

> Use of our products and services has and may involve the transmission and/or storage of data, including in certain instances our own and our customers' and other parties' business, financial and personal data. As we continue to evolve our products and features, we expect to host, transmit or otherwise have access to increasing amounts of potentially sensitive data. Maintaining the security of our products, computer networks and data storage resources is important and service vulnerabilities could result in loss of and/or unauthorized access to confidential information.
>
> …
>
> As a more general matter, unauthorized parties may attempt to misappropriate, alter, disclose, delete or otherwise compromise our confidential information or that of our employees, partners, customers or their end users, create system disruptions, product or service vulnerabilities or cause shutdowns.
>
> …
>
> These misappropriations, cyberattacks or any other compromises of our security measures (or those of one of our customers) as a result of third-party action, malware, employee error, vulnerabilities, theft, malfeasance or otherwise could result in (among other consequences):
>
> …
>
> - individual and/or class action lawsuits, due to, among other things, the compromise of sensitive employee or customer information, which could result in financial judgments against us or the payment of settlement amounts and cause us to incur legal fees and costs;
>
> - regulatory enforcement action in the United States at both the federal and state level (such as by the Federal Trade Commission and/or state attorneys general) or globally under the growing number of data protection legal regimes, including without limitation the General Data Protection Regulation, or GDPR, and the California Consumer Privacy Act, or CCPA, or other similar

[29] *Citrix Systems, Inc. 2021 Annual Report on Form 10-K*, SEC (Feb. 16, 2022), https://www.sec.gov/Archives/edgar/data/877890/000087789022000019/ctxs-20211231.htm.

> federal, state or local laws, which could result in significant fines and/or penalties or other sanctions and which would cause us to incur legal fees and costs;
>
> - costs associated with responding to those impacted by such issues, such as: costs of providing data owners, consumers or others with notice; legal fees; costs of any additional fraud detection activities required by such customers' credit card issuers; and costs incurred by credit card issuers associated with the compromise;
>
> - disputes with our insurance carriers concerning coverage for the costs associated with responding to, and mitigating an incident; and/or
>
> - longer-term remediation and security enhancement expenses.

60. Citrix also represents that the NetScaler Products will allow its customers like Comcast (and its employees) "to securely access their virtual desktops and applications from anywhere, on any device, and across any network."[30]

61. In the "Citrix Trust Center" on Citrix's website, Citrix emphasizes that customers' "security is our priority," noting that "[r]esponsibly adopting advanced technologies requires a critical eye on cybersecurity and data privacy. Because we design our products around centralized delivery, visibility and control of apps and data, security is built into the core of our solutions and practices."[31]

62. Elsewhere on the Trust Center webpage, Citrix markets its ability to keep customers' data secure, stating: "For almost 30 years, our customers have trusted our ability to handle their data with care and respect. That's why organizations from the most highly regulated sectors rely on us to protect their most sensitive information wherever work happens."[32]

---

[30] *Secure Access for Citrix DaaS Use Cases*, NETSCALER, https://www.citrix.com/solutions/improving-application-performance-and-security.html (last visited Mar. 20, 2025).
[31] *Citrix Trust Center*, Citrix, https://www.citrix.com/about/trust-center/ (last visited Mar. 20, 2025).
[32] *Privacy & Certifications*¸ Citrix, https://www.citrix.com/about/trust-center/privacy-compliance.html (last visited Mar. 20, 2025).

63. Similarly, the privacy policy for Cloud Software Group, Inc., states that Citrix protects personal information by "maintain[ing] administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Personal Information."[33]

64. As part of its function to deliver a secure infrastructure, the NetScaler Products were fitted with certain cybersecurity features like "Cookie Consistency Check." If enabled and properly configured and managed, this NetScaler cybersecurity feature could have narrowed the scope of the Data Breach.

65. Cookie Consistency Check can be used to ensure session integrity, i.e., verifying that a user with an active session is actually who they claim to be. Specifically, this feature ensures that cookies are correctly tied to the session and have not been tampered with (i.e., it is not hijacked). Thus, if an attacker tried to manipulate the session cookie (for example, to hijack an existing session), the consistency check would have identified that the cookie did not match the expected session and prevented unauthorized access, if properly configured and managed.

66. Cookie Consistency Check was available at the time of the Data Breach. The fact that cybercriminals were able to send requests from a legitimate user's session despite having a different IP address signals that Comcast did not enable the Cookie Consistency Check cybersecurity feature on its NetScaler Products or that Comcast did not properly configure and/or manage this feature. This is one of many ways Comcast failed Plaintiff and Class Members.

67. After the Data Breach, Citrix released a new security feature called, "Cookie hijacking protection." This feature works similarly to the Cookie Consistency Check but is purportedly less complex to use. Citrix was aware of that complexity but waited until after the

[33] *Privacy Statement*, Cloud Software Group (May 7, 2024), https://www.cloud.com/privacy-policy.

Data Breach to introduce this new feature. Indeed, in a video highlighting the new feature, Citrix acknowledged that this hijacking protection was previously offered but used a more complex method.[34] Had Citrix decided to release this hijacking protection feature earlier (as it knew its existing features were complex to implement), it would have been more likely that companies like Comcast could have used this hijacking protection feature to lessen the scope of the Data Breach.

68. At all relevant times, Citrix was aware that its NetScaler Products were used to protect access to sensitive PII, and as such had a responsibility to provide secure remote infrastructure for its clients. Citrix was equally aware of the foreseeable risks associated with the exploitation of vulnerabilities in its purportedly secure infrastructure.

D. Defendants' Legal Responsibility to Safeguard Information.

69. Beyond the obligations created in their security and privacy policies and other promises made to consumers about the security of their data, Comcast and Citrix owed Plaintiff and Class Members a legal duty to safeguard their PII.

70. First, as described further below, Comcast and Citrix owed a duty to safeguard PII pursuant to several federal and state statutes, including the Federal Trade Commission Act ("FTC Act") and the Cable Communications Policy Act, to ensure that all information collected and stored was secure. These statutes were intended to protect Plaintiff and Class Members from the type of conduct by Comcast and Citrix alleged herein.

71. Comcast also owed a nondelegable duty to safeguard PII given that Comcast knew that it was maintaining highly valuable data, for which Comcast knew would be targeted by cybercriminals. Comcast likewise knew of the extensive harm that would occur if Plaintiff's and

[34] *Live Demo: NetScaler Live Demo | Session hijack protection for NetScaler Gateway/AAA deployments* available at: https://youtu.be/isVkw9Q2KkU?si=QQyR56a7RRr_lFTM&t=678.

Class Members' PII were exposed through a Data Breach, and thus owed a nondelegable duty to safeguard that information.

72. Citrix similarly was well-aware that its products were used by customers that handled sensitive PII, and as such knew that any vulnerabilities in its products could lead to the access, compromise, and theft of PII.

73. Given the sensitive nature of the PII obtained by the cybercriminals in the Data Breach, Comcast knew that these hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, social engineering attacks, and other identity-related fraud if they were able to exfiltrate the PII from Comcast's system. Comcast also knew that individuals whose PII was stored on Comcast's servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated. Indeed, in its notice letter, Comcast expressly acknowledged, recognized, and appreciated the imminent threat and substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that consumers could take certain actions like monitoring their financial accounts and credit reports.

74. Citrix similarly recognized that, given its customers used its products to store and manage PII, any breach of those products' security vulnerabilities would result in identity theft, financial fraud, phishing, social engineering attacks, and other identity-related fraud. Citrix also knew that individuals whose PII was stored on its customers' systems would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

75. Comcast also owed a duty to safeguard Plaintiff's and Class Members' data based upon the promises that it made to its customers to safeguard data, as well as the disclosures that it

made in its data security policies, privacy policies, and SEC filings. Comcast undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiff and Class Members to keep their PII secure.

76. Citrix similarly owed a duty to safeguard Plaintiff's and Class Members' data based upon the promises that it made to its customers regarding its products' ability to safeguard data, as well as the disclosures that it made in its data security policies, privacy policies, and SEC filings. Citrix undertook efforts to keep customers' data secure as part of its business model and thus owes a continuing obligation to Plaintiff and Class Members to keep their PII secure.

77. Citrix also owed a duty because its affirmative conduct created a foreseeable risk of harm to Plaintiff and Class Members. Citrix's affirmative act in announcing the Citrix Bleed vulnerability to the public without exercising reasonable care by simultaneously releasing full and complete patching guidance (and ultimately not releasing full and complete guidance until nearly two weeks later) gives rise to a duty to Plaintiff and Class Members who are the foreseeable victims, as Citrix knew that Plaintiff and Class Members would be likely harmed as a result of its conduct.

78. Comcast and Citrix each also owed a duty to comply with industry standards in safeguarding PII, which—as discussed herein—neither company complied with.

E. Defendants Knew the Risks of Collecting and Storing Valuable PII and the Foreseeable Harms of Exposing PII to Cybercriminals.

79. At all relevant times, Comcast knew it was storing and collecting customers' sensitive PII, and, that as a result, those systems would be attractive targets for cyber criminals.

80. Similarly, at all relevant times, Citrix knew that its NetScaler Products would be used by companies like Comcast to provide a secure remote connection to these companies'

internal networks, thereby preventing cybercriminals from gaining access to their computer systems and networks.

81. The data that Comcast stores and utilizes Citrix NetScaler to protect is a treasure trove for cyber criminals as this data contains all of the necessary building blocks to commit fraud. Indeed, the PII that customers entrusted to Comcast includes usernames and hashed passwords, names, contact information, Social Security numbers, driver's license numbers, dates of birth, and secret security questions and answers.

82. The ramifications of Defendants' failure to protect Plaintiff's and the Class's PII are long lasting and severe, particularly given the risk of identity theft that Plaintiff and the Class now face. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

83. The Federal Trade Commission recognizes identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[36]

84. PII, including the information collected by Comcast, is highly valued by criminals, as evidenced by the prices that such information commands on the dark web. Numerous sources

[35] 17 C.F.R. § 248.201 (2013).
[36] *Id.*

cite dark web pricing for stolen identity credentials. For example, a single victim's personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[37] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[38]

85. Moreover, there may be a time lag between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

86. Moreover, the telecommunications industry is "among the most-targeted sectors globally for cybercriminals, and it's not hard to see why. Sensitive user information is carried at a massive scale on telecom networks, and that naturally makes them an attractive target for malicious actors."[40] Indeed, there have been numerous high-profile data breaches in the telecommunications industry in recent years, including Comcast, T-Mobile, and AT&T.

---

[37] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

[38] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[39] Report to Congressional Requesters, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

[40] Katy, Allan, *The growing concerns in telecommunication cybersecurity*, Cyber Magazine (Oct. 30, 2023), https://cybermagazine.com/articles/the-growing-concerns-in-telecommunication-cybersecurity.

87. The breadth of the data compromised in the Data Breach also makes the information particularly valuable to cybercriminals and leaves Comcast's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

88. **Social Security Numbers**—An individual's Social Security number is made up of three parts: (1) an area number (the first three digits); (2) a group number (the middle two digits); and (3) a serial number (the last four digits). The area number corresponds to the state in which an individual applied for their Social Security number, while the group number refers to the specific order in which Social Security numbers are distributed within a geographical region. Finally, the serial number corresponds with the area and group number and is designed to distinguish one Social Security number from the next.[41] Thus, the last four digits is the only unique part of a person's Social Security number and is used to identify that person.

89. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

90. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state

[41] *Structure of Social Security Numbers*, Barcodes, https://www.barcodesinc.com/articles/structure-of-social-security-numbers.htm (last visited Mar. 20, 2025).

> motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[42]

91. The last four digits of Social Security numbers are commonly used in identity verification processes across various sectors, including financial institutions, healthcare providers, and government agencies. Cybercriminals exploit this reliance by combining these digits with other personal information to bypass security measures. For instance, the Federal Trade Commission warns against sharing even partial Social Security numbers, as scammers can use them to commit identity theft.[43] The theft of the last four digits of an individual's Social Security number can thus subject them to identity theft and fraud as companies and creditors often verify someone's identity by asking only for the last four digits, or the "serial number," of an individual's Social Security number. As such, cyber criminals armed with the last four digits of an individual's Social Security number, in combination with other personal information—as is the case here—can open accounts, access an individual's name, or apply for benefits in that person's name.[44]

---

[42] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[43] *Fake calls about your SSN*, Fed. Trade Comm'n (Dec. 12, 2018), https://consumer.ftc.gov/consumer-alerts/2018/12/fake-calls-about-your-ssn.
[44] Hari Ravichandran, *What Can Someone Do With Your Social Security Number*, Aura (Apr. 8, 2024), https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number#:~:text=Many%20banks%2C%20government%20agencies%2C%20and,for%20benefits%20in%20your%20name.

92. Cybercriminals can also use computer programs to easily predict the first five digits of an individual's Social Security number, thus allowing them to determine an individual's full nine-digit number and commit even more types of fraud. A study revealed that knowing an individual's birth date, place, and last four digits of their Social Security number can lead to an accurate prediction of their full Social Security.[45] This predictability poses significant risks to victims of data breaches such as this one, as it enables criminals to reconstruct full Social Security numbers from partial data.

93. Even without the first five digits of a Social Security number, partial Social Security numbers can be used as part of a strategy to gain access to a victim's accounts or credit. Credential stuffing involves using stolen credentials to gain unauthorized access to multiple accounts. Partial Social Security numbers are valuable in such attacks, as they can be used to bypass security questions or as part of multi-factor authentication processes. Social engineering schemes also leverage partial Social Security numbers to build trust with victims or customer service representatives, facilitating unauthorized access.[46]

94. Government agencies consider the last four digits of Social Security numbers to be highly sensitive PII, "both stand-alone and when associated with any other identifiable information," that requires special considerations when being electronically transmitted.[47] The

[45] Alessandro Acquisti & Ralph Gross, *Predicting Social Security numbers from public data*, PNAS (July 7, 2009), https://www.pnas.org/doi/10.1073/pnas.0904891106.Xeni Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), https://boingboing.net/2009/07/06/reverse-engineering.html.
[46] *The Importance of Protecting the Last Four Digits of Your Social Security Number*, Robinson+Cole (Sept. 18, 2018), https://www.dataprivacyandsecurityinsider.com/2018/09/the-importance-of-protecting-the-last-four-digits-of-your-social-security-number/.
[47] *Frequently Asked Questions (FAQ)*, U.S. Dep't of Commerce, Office of Privacy and Open Government, https://www.commerce.gov/opog/frequently-asked-questions-faq (last visited Mar. 20, 2025).

Department of Homeland Security emphasizes the importance of safeguarding even partial Social Security numbers to prevent unauthorized access.[48] Because loss of "[t]he full or partial SSN can increase the risk of identity theft or fraud (i.e., access to bank accounts, driving records, tax and employment histories, and other private information," NIH recommends the following[49]:

- Collect SSN as a primary identifier only if permitted by law;
- Reduce and/or eliminate the use of SSNs not required for a business purpose;
- Use an alternate identifier (unique, randomly generated number not derived from PII); and
- Transmit SSN electronically only through an encrypted means.

95. Unlike usernames and passwords, Social Security numbers are permanent identifiers that cannot be easily changed. This permanence means that once a Social Security number is exposed, the individual is at risk of identity theft indefinitely. Victims of identity theft from data breaches often face multiple incidents of fraud over their lifetime due to the reuses of stolen data, and "may not find out that someone is using your [Social Security number] until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought,"[50] which highlights the long-term risks of stolen full or partial Social Security numbers.

96. **Usernames and Passwords**—When cybercriminals gain access to an individual's username and password for one account, cybercriminals gain access to the username and password

[48] *Handbook for Safeguarding Sensitive PII*, U.S. Dep't of Homeland Security (Dec. 4, 2017), https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.
[49] *The Privacy Pulse*, U.S. Nat'l Inst. Health (June 21, 2013), https://oma.od.nih.gov/forms/Privacy%20Documents/Privacy%20Newsletters/2013/Privacy%20Pulse%20-%20June%202013%20SSN.pdf.
[50] *Identity Theft and Your Social Security Number*, Social Security Administration (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

for an individual's other accounts, as well. Research has indicated that individuals typically reuse passwords on ten of their personal accounts and that more than six in ten people have admitted to reusing passwords. When these studies are combined with studies that suggest that more than 80% of confirmed breaches are related to stolen, weak, or reused passwords, the compromise of an individual's username and password in one data breach provides cybercriminals with the ammunition needed to wreak havoc on an individual's other accounts.[51]

97. **Security Questions and Answers**—Security questions and answers are also dangerous in the hands of cybercriminals. Security questions and answers which often involve supposedly "secret" information like a consumer's favorite place to travel or the street on which the consumer grew up, are frequently utilized by cybercriminals to reset an individual's password and thereby gain access to their account. Because security questions are commonly repeated across various websites, often involving things like an individual's mother's maiden name, the city in which they were born, or an individual's first pet, they are reused across many accounts, and their compromise in one data breach will lead to the compromise across many other accounts, subjecting an individual to a single point of compromise across all accounts.[52]

98. Even if cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

[51] Clare Stouffer, *139 password statistics to help you stay safe in 2024*, Norton (June 27, 2023), https://us.norton.com/blog/privacy/password-statistics.
[52] Lily Hay Newman, *Time to Kill Security Questions—or Answer Them With Lies*, Wired (Sept. 28, 2016), https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/.

99. The development of "Fullz" packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers is not included in the PII stolen in a specific incident, criminals can easily create a "Fullz" package that links that information together and sell the package at a higher price.

100. Importantly, once a cybercriminal has a "Fullz" package, cybercriminals can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[53] Most problematic, however, is that cybercriminals in possession of a "Fullz" package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[54]

101. The PII compromised in the Data Breach is also valuable to cybercriminals because it can be used to commit "porting-out" scams, whereby cybercriminals use different methods to highjack an individual's phone number, assume their identity, intercept security protocols sent to an individual's phone, and gain access to their financial and social media accounts.[55]

102. In a port-out scam (or a similar "SIM-swap" scam), as explained by the FTC, cybercriminals will target an individual's PII, including their name, address, birth date, PINs, passwords, and the last four digits of their Social Security number to initiate a port request with the individual's phone company. Specifically, cybercriminals can use the PII compromised in the

[53] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DataDome (Mar. 3, 2023), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work.
[54] *Protection Against Fullz and Fraud, Integrity*, Aristotle (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.
[55] *Port-Out Fraud Targets Your Private Accounts*, Federal Trade Comm'n (Nov. 17, 2023), https://www.fcc.gov/port-out-fraud-targets-your-private-accounts.

Data Breach to scam an individual's phone company into porting the individual's phone number to a different mobile device or a service account set up by the cybercriminal. Once the cybercriminal's porting request is successful, the cybercriminal begins receiving the individual's private texts and calls, can reset the access credentials for many financial and social medial accounts as text messages are frequently used by businesses to verify an individual's identity, and subsequently drain the victim's accounts or ransom back access to the victim's accounts.[56]

103. To protect against port-out and SIM-swap scams, the FTC advises individuals to guard against personal details that can be used to verify their identity, including the last four digits of their Social Security numbers, their phone numbers, their dates of birth, the make and model of their cars, their pet's name, and their mother's maiden name—the very PII that was compromised in the Data Breach and now in the hands of cyber criminals.[57]

104. Comcast is aware of port-out and SIM-swap scams and even provides a form on their website for customers to report potential scams.[58]

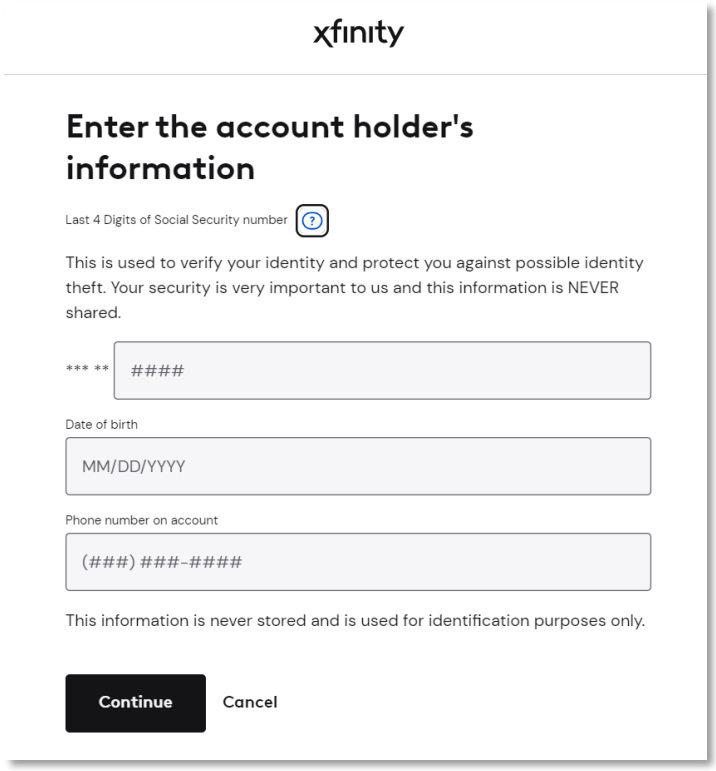
105. Furthermore, the PII acquired in the Data Breach is valuable to cybercriminals because it is tied to Comcast. Cybercriminals can exploit (and already have exploited) the trust and relationship between Plaintiff and Class Members and Comcast. In addition to the port-out fraud described above, cybercriminals can now use the PII acquired in the Data Breach to craft more personalized phishing emails or social engineering attempts, substantially increasing the likelihood of identity theft and fraud.

---

[56] *Id.*
[57] *Id.*
[58] *Fraudulent Activity Reporting*, Xfinity, https://www.xfinity.com/support/account-management/sim-port-fraud-reporting (last visited Mar. 20, 2025).

106. Indeed, Class Members have already received emails from accounts purporting to be Comcast/Xfinity, informing Plaintiff and Class Members, among other things, that they "have been chosen to participate in [Comcast's] Loyalty Program" or that there is a problem with their "payment method on file." These emails appear to originate from Comcast/Xfinity and attempt to trick the recipient into clicking a malicious link.

107. Finally, the PII acquired by cybercriminals in the Data Breach is the same data used for a Comcast/Xfinity customer to access their Xfinity account. At the time of the Data Breach, as an alternative means of accessing one's Comcast account, Comcast allowed its customers to authenticate themselves with the last four digits of their Social Security number, date of birth, and phone number on the account—all of which is information compromised in the Data Breach, as shown below.[59]



[59] The below picture is a screenshot of Comcast's authentication webpage as recent as October 2024. However, Comcast recently removed the ability to authenticate using a customer's last 4

108. Comcast acknowledges the significance of the last four digits of a Social Security number. As demonstrated in the picture above, Comcast represents that a customer's last four digits of their Social Security number "is used to verify your identity and protect you against possible identity theft." Comcast also represents that customers' "security is very important to us," and the last four digits of customers' Social Security numbers are "NEVER shared." Comcast promises that "[t]his information is never stored and is used for identification purposes only." Thus, Comcast fully appreciated and understood the sensitivity of the last four digits of Social Security numbers. Cybercriminals with this information can access Plaintiff's and Class Members' Comcast accounts and acquire even more data, such as bank information on file and purchases/subscriptions, which reveal viewing habits and other personal decisions, by Plaintiff and Class Members.

109. Aside from these risks of identity theft and fraud, PII is also property that has monetary value to data breach victims.

110. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[60]

---

digits of their Social Security number, date of birth, and phone number. The initial authentication landing page, which notes the ability to authenticate one's account using a Social Security number, remains available via the Internet Archive at https://web.archive.org/web/20230601001851/https://idm.xfinity.com/myaccount/lookup?execution=e1s1. The current version of this webpage is available at https://idm.xfinity.com/myaccount/.

[60] Brad Brown et al., *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/capabilities/quantumblack/our-insights/capturing-value-from-your-customer-data.

111. In 2013, the Organization for Economic Cooperation and Development ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[61] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[62]

112. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [$2] for a date of birth, USD 8 [$8] for a Social Security number (government ID number), USD 3 [$3] for a driver's license number and USD 35 [$35] for a military record. A combination of address, date of birth, Social Security number, credit record and military [record] is estimated to cost USD 55 [$55]."[63]

113. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee-for-services-provided to monetizing their users' data—including user data that is not necessary for product or service, which she refers to as "behavioral surplus."[64]

114. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to users. Market exchanges have sprung up where individual users like Plaintiff can sell or monetize their

[61] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[62] *Id.* at 25.
[63] *Id.*
[64] Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[65] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[66]

115. There are numerous examples of this kind of market, which is growing more robust as information asymmetries are diminished when users discover how their data is being covertly intercepted, collected, used, and disclosed.

116. As a group of information technology professors relayed in a 2016 article entitled "The Economics of Privacy," published in the Journal of Economic Literature:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, and consumption habits) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[67]

117. In other words, a successful cyberattack leaves criminals with a lucrative and readily monetized supply of PII—and deprives its victims of the exclusive use of their own information.

118. The documented increase in cyberattacks, combined with increasing monetary incentives that heighten the risk of future attacks, was widely known to the public and to anyone in Defendants' industries, including Defendants, at the time of the Data Breach.

119. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the telecommunications industry preceding the date of the Data Breach.

---

[65] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.
[66] Jacob Kastrenakes, *A new TikTok Clone hit the top of the App Store by paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival.
[67] Alessandro Acquisti et al., *The Economics of Privacy*, 54 J. of Econ. Lit. 442, 444 (June 2016).

120. Plaintiff and Class Members, as current and former customers of Comcast, relied on both Comcast and Citrix to keep their PII confidential and secure, to use their information for business purposes only, and to make only authorized disclosure of their information.

121. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Comcast assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from foreseeable risks of disclosure to unauthorized parties. Comcast agreed to and undertook legal duties to securely store and maintain the PII of Plaintiff and Class Members.

122. Similarly, by providing Comcast with NetScaler products to protect Plaintiff's and Class Members' PII, Citrix assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from foreseeable risks of disclosure to unauthorized parties.

F. Despite Their Duties and the Foreseeable Risk of Harm, Comcast and Citrix Failed to Protect Plaintiff's and Class Members' PII.

123. At the same time Comcast collected, stored, and profited from Plaintiff's PII using Citrix technology—and while Comcast was actively promising consumers that "we're always working to keep your personal information secure" and Citrix was telling customers like Comcast that they could rely on Citrix's products to "deliver the applications and data employees need across any network with security, reliability and speed"—cybercriminals exploited a vulnerability in Citrix's products and stole nearly 36 million current and former Comcast customers' PII.

124. On October 10, 2023, Citrix published a security bulletin entitled "NetScalerADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967" that announced: "Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix

ADC) and NetScaler Gateway (formerly Citrix Gateway)."[68] The bulletin noted that the vulnerabilities at issue affected a wide array of ADC and NetScaler Gateway products, and directed any entity using "customer-managed" NetScaler ADC and NetScaler Gateway products to take action to fix those vulnerabilities.

125. Citrix's security bulletin rated CVE-2023-4966 at 9.4 out of 10 on the Common Vulnerability Scoring System (CVSS). This designates the vulnerability as "Critical"—meaning it "[h]as a severe impact, create[ing] immediate and big risks."[69]

126. The CVE-2023-4966 vulnerability has become known in the cybersecurity community as "Citrix Bleed," and allows cybercriminals to gain unauthorized access to sensitive data contained on internal systems.[70] Specifically, an attacker exploiting Citrix Bleed sends a specially crafted HTTP GET request to a vulnerable NetScaler appliance API, which sends back a cache of information from which a session cookie can be extracted. This session cookie then allows a cybercriminal to hijack a legitimate user's existing, authenticated session with the NetScaler appliance without any need for a username, password, or multi-factor authentication token or device.[71] In other words, cybercriminals exploiting Citrix Bleed hijacked legitimate users' already-active sessions.

127. The federal Cybersecurity & Infrastructure Security Agency (CISA) shortly thereafter issued a cybersecurity advisory regarding the Citrix Bleed vulnerability, stating:

---

[68] Citrix Bleed Security Bulletin, *supra* note 3.
[69] Mars Groves, *Understanding CVSS: The Common Vulnerability Scoring System*, Fossa (Nov. 7, 2024), https://fossa.com/blog/understanding-cvss-common-vulnerability-scoring-system.
[70] *Citrix Bleed, a vulnerability in massive exploitation phase*, Telefónica Tech (Dec. 4, 2023), https://telefonicatech.com/en/blog/Citrix Bleed-a-vulnerability-in-massive-exploitation-phase.
[71] *Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966),* Mandiant (Oct. 31, 2023), https://cloud.google.com/blog/topics/threat-intelligence/session-hijacking-citrix-cve-2023-4966/.

> Citrix Bleed, known to be leveraged by LockBit 3.0 affiliates, allows threat actors to bypass password requirements and multifactor authentication (MFA), leading to successful session hijacking of legitimate user sessions on Citrix NetScaler web application delivery control (ADC) and Gateway appliances. Through the takeover of legitimate user sessions, malicious actors acquire elevated permissions to harvest credentials, move laterally, and access data and resources.[72]

128. Despite learning on October 10, 2023, of the Citrix Bleed vulnerability that was ultimately exploited in the Data Breach, Comcast waited an unreasonable amount of time to initiate implementation of the security patch.

129. To downplay the severity of the Data Breach and Comcast's unreasonable delay, Comcast later told customers that it "promptly patched and mitigated [its] systems."[73] Unfortunately for Comcast customers including Plaintiff and Class Members, Comcast's failure to promptly patch its systems allowed the Data Breach to occur. The unreasonable delay caused Plaintiff and the Class Members irreparable harm not only because of the initial breach, but also because by failing to timely and promptly notify Plaintiff and the Class Members, Defendants prevented Plaintiff and Class Members from taking precautionary measures, leading many of them to become victims of identity theft and fraud.

130. The specific exploitation of Citrix Bleed that resulted in the Data Breach was sophisticated, intentional, and targeted. After cybercriminals discovered the Citrix Bleed vulnerability, cybercriminal gangs rapidly developed custom scripts in numerous simple

---

[72] *#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability*, CISA (Nov. 21, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a.

[73] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited Mar. 20, 2025).

programming languages that could exploit NetScaler gateway devices to extract session cookies.[74] Threat actors, particularly Lockbit 3.0 affiliates, used these scripts to automatically search for, find, and exploit NetScaler devices across the Internet, first targeting high-value network infrastructure providers such as Comcast from which they could extract valuable consumer PII.[75] Use of these scripts to hack Comcast's NetScaler products demonstrates that the cybercriminals behind the Data Breach intentionally sought out Comcast's networks to extract customers' PII.

131. Comcast knew (or should have known) that time was of the essence to implement the patch after it learned of the vulnerability on October 10, 2023, because it is well established that cybercriminals quickly act on any vulnerabilities, in some cases as little as 15 minutes after the vulnerability is announced.[76]

132. Comcast failed to act quickly, however. An unreasonable amount of time transpired from the time that Comcast learned of the vulnerability to the time when the Data Breach occurred, which was more than enough time for Comcast to patch the vulnerability. Had Comcast timely implemented the patch on October 10, 2023, or in the five days following, it could have prevented the Data Breach entirely.

---

[74] *#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability*, CISA (Nov. 21, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a. An example of Citrix Bleed exploit code written in Python is available at: https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-4966.

[75] Sam Sabin, *The security flaw haunting cyber defenders in 2024*, Axios (Jan. 2, 2024), https://www.axios.com/2024/01/02/citrix-bleed-security-hacks-impact.

[76] Zak Islam, *Hackers now exploit new vulnerabilities in just 15 minutes*, Digitaltrends (July 27, 2022), https://www.digitaltrends.com/computing/hackers-now-exploit-new-vulnerabilities-in-just-15-minutes/; Bill Toulas, *Hackers use PoC exploits in attacks 22 minutes after release*, BleepingComputer (July 13, 2024), https://www.bleepingcomputer.com/news/security/hackers-use-poc-exploits-in-attacks-22-minutes-after-release/; Patrick Pocalyko, *With CVEs, time is on hackers' side*, Security (Dec. 12, 2023), https://www.securitymagazine.com/articles/100238-with-cves-time-is-on-hackers-side; TrustNet, *Cybercriminals are getting faster at exploiting vulnerabilities*, https://trustnetinc.com/cybercriminal-are-getting-faster-at-exploiting-vulnerabilities/.

133. Through these failings, Comcast granted cybercriminals unfettered access to its systems and Plaintiff's and Class Members' sensitive information and allowed the Data Breach to transpire undetected for three consecutive days.

134. Comcast's failures in preventing the Data Breach and mitigating the Data Breach once it started are therefore numerous, as partially summarized below:

a. First, Comcast should have noticed that the IP addresses used by the cybercriminals were neither active nor routable within the Comcast network, which should have alerted Comcast security to potentially malicious activity, as inactive IP addresses are often used by threat actors.[77] That Comcast failed to note inactive IP addresses suddenly becoming active indicates inadequate cybersecurity practices.

b. Second, Comcast should have employed "application whitelisting" to prevent the installation of certain tools commonly used by cybercriminals to carry out data breaches. Application whitelisting is a security practice that allows only pre-approved and trusted applications to run on a system, blocking any unauthorized or unknown software from executing.[78] The National Institute of Standards and Technology NIST 800-167 recommends application whitelisting.[79]

[77] Patrick Kinsley, *Unused IP addresses: What are the Cybersecurity Risks*?, SparkNav (May 28, 2024), https://sparknav.com/insights/unused-ip-addresses-what-are-the-cybersecurity-risks/.
[78] Katie C. Stewart, *Establish and Maintain Whitelists*, Carnegie Mellon Univ. (Oct. 25, 2017), https://insights.sei.cmu.edu/blog/establish-and-maintain-whitelists-part-5-of-7-mitigating-risks-of-unsupported-operating-systems/.
[79] Adam Sedgewick et al., *Guide to Application Whitelisting*, NIST (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf

c. Third, Comcast failed to ensure that only specific users with specific privileges, such as administrators, were able to install software on a system.[80] This is part of the fundamental cybersecurity concept of the principle of least privilege (PoLP), which dictates that users, applications, systems, or processes should be granted only the minimum levels of access—or permissions—necessary to perform their specific tasks. By limiting access rights, organizations can reduce the potential attack surface, mitigate the risk of accidental or intentional misuse of privileges, and enhance overall system security. Each user or process receives only the permissions essential for their function, preventing unnecessary access to sensitive data or critical system components.[81] NIST SP 800-53 emphasizes least privileges as follows:

> The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design.[82]

---

[80] MITRE ATT&CK, *Mitigations: Limit Software Installation*, https://attack.mitre.org/mitigations/M1033/.

[81] Fred B. Schneider, *Least Privilege and More*, IEEE Security & Privacy (Sept. 2003), https://www.cs.cornell.edu/fbs/publications/leastPriv.pdf; *About the Principle of Least Privilege*, Ind. Univ. Knowledge Base, https://servicenow.iu.edu/kb?id=kb_article_view&sysparm_article=KB0022770.

[82] *Security and Privacy Controls for Information Systems and Organizations*, NIST, https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

If Comcast had complied with the foregoing best practices and industry standards, and simply restricted software installation to administrator accounts, the Data Breach would not have occurred or would have been mitigated.

d. Fourth, Comcast's system should have notified someone, such as a security administrator, whenever new software is installed, even if the software is whitelisted and the user has appropriate privileges to install the software.[83]

135. Comcast has more than sufficient resources to prevent this Data Breach and was aware of, and could have implemented, the simple actions and measures listed in subparts (a) through (d) above, which would have either prevented the Data Breach entirely, or at least alerted Comcast security immediately at the very earliest stages of the Data Breach (thereby substantially reducing its scope and harm imposed). For example, Comcast advertises cybersecurity services to other businesses.[84] Comcast also advertises that it internally uses DataBee and BlueVector products to "gain real-time compliance trends and mitigate and stop threats."[85] Comcast further advertises its own cybersecurity products with phrasing such as "[o]ne breach has the potential to dramatically impact your business — and customers. Comcast Business SecurityEdge™ helps protect all connected devices on your network from malware, phishing scams, ransomware, and

[83] Peter Barnett, *How to Monitor All Software Installation to Prevent Data Breaches,* Action1 (Oct. 18, 2018), https://www.action1.com/how-to-monitor-all-software-installation-to-prevent-data-breaches-action1/.
[84] Comcast Business, *Cybersecurity Services*, https://business.comcast.com/enterprise/products-services/cybersecurity-services.
[85] Comcast Technology Solutions, https://www.comcasttechnologysolutions.com/databee-suite.

botnet attacks."[86] Furthermore, Comcast publishes annual cybersecurity threat reports.[87] Comcast also has its own cybersecurity research team.[88]

136. Citrix is equally blameworthy for this Data Breach. For example, Citrix did not discover the existence of Citrix Bleed in a timely manner. Mandiant, a leading cybersecurity and threat intelligence firm that is a subsidiary of Google, identified exploitation of the Citrix Bleed vulnerability "in the wild" beginning in August of 2023, based on its discovery of "multiple instances of successful exploitation of CVE-2023-4966 that resulted in the takeover of legitimate user sessions on NetScaler ADC and Gateway appliances."[89] Mandiant discovered these exploitations prior to October 10, 2023, while it was "conducting investigations where a threat actor was taking over user's NetScaler sessions through unknown means."[90] Citrix thus either knew or should have known that its NetScaler Products were actively being exploited earlier than October 10, 2023.

137. Mandiant's investigation into the Citrix Bleed vulnerability demonstrated the risks that come from widespread use of Citrix's NetScaler products. According to Mandiant, exploitation of the Citrix Bleed vulnerability occurred across many sectors, as Mandiant itself was investigating breaches related to Citrix Bleed exploitation in "legal and professional services, technology, and government organizations." Additionally, Mandiant suspected that "the number

[86] Comcast Business, *SecurityEdge*, https://business.comcast.com/learn/internet/security-edge.
[87] Comcast Business, *Cybersecurity Insights*, https://business.comcast.com/community/cybersecurity.
[88] Comcast Cyber Security Research, https://corporate.comcast.com/ccs-research.
[89] *Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966),* Mandiant (Oct. 31, 2023), https://cloud.google.com/blog/topics/threat-intelligence/session-hijacking-citrix-cve-2023-4966/.
[90] *Id.*

of impacted organizations is far greater" and occurred in even more sectors, "[g]iven the widespread adoption of Citrix in enterprises globally."[91]

138. Indeed, prior to the Data Breach, Comcast and Citrix knew or should have known that Citrix NetScaler applications had an array of vulnerabilities and a lack of security protocols that made it dangerous and extremely risky to use NetScaler to store any sensitive information. For example, in July 2023 a zero-day vulnerability in Citrix ADC and NetScaler Gateway appliances (CVE-2023-3519) was discovered, which enabled remote code execution by threat actors, and which was exploited by China-based threat actors with a known history of targeting Citrix ADCs.[92] And in late 2022, two separate vulnerabilities in Citrix ADC and Gateway appliances were discovered (CVE-2022-27510 and CVE-2022-27518), which allowed unauthenticated threat actors to gain unauthorized access to devices and Citrix servers—much like in the Data Breach at issue here.[93] The fact that there had been recent vulnerabilities in Citrix products, specifically the same products affected by CVE-2023-4966, should have alerted Citrix and Comcast to diligently monitor these products for security flaws.

139. Along with a belated disclosure of the vulnerability, Citrix also initially failed to reveal the severity of the vulnerability. While Citrix originally recommended "customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions" of the NetScaler

---

[91] *Id.*

[92] James Nugent et al., *Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)*, Mandiant (Jul. 21, 2023), https://cloud.google.com/blog/topics/threat-intelligence/citrix-zero-day-espionage.

[93] Bill Toulas, *Thousands of Citrix servers vulnerable to patched critical flaws*, BleepingComputer (Dec. 28, 2022), https://www.bleepingcomputer.com/news/security/thousands-of-citrix-servers-vulnerable-to-patched-critical-flaws/

products "as soon as possible,"[94] it was not until a week later that Citrix revealed—in bold and underlined font—that "**[e]xploits of CVE-2023-4966 on unmitigated appliances have been observed.**"[95] And six days after that, Citrix finally recommended that those using the NetScaler products "kill[] all active and persistent sessions[.]"[96]

140. Moreover, Citrix's initial disclosure of the Citrix Bleed vulnerability did not reference terminating all active sessions after applying the patch, even though it knew that an exploit of Citrix Bleed would use compromised session cookies to breach a vulnerable NetScaler Product.

141. Indeed, many companies failed to timely deploy the Citrix patches, which, on information and belief, was due to the lack of urgency and severity communicated in the initial Citrix bulletin. For example, one analysis in December 2023 found that roughly 4,600 vulnerable Citrix products were still online as of October 31, 2023, and 1,300 vulnerable products remained online by December 31, 2023.[97] And while many companies timely patched their Citrix products and prevented a breach of their systems, several large companies beyond Comcast were also

[94] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix (Oct. 10, 2023), https://web.archive.org/web/20231012010221/https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967/.
[95] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix (Oct. 17, 2023), https://web.archive.org/web/20231018100605/https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967.
[96] Anil Shetty, *CVE-2023-4966: Critical security updated now available for NetScaler ADC and NetScaler Gateway* (Oct. 23, 2023), https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/.
[97] Sam Sabin, *The security flaw haunting cyber defenders in 2024,* Axios (Jan. 2, 2024), https://www.axios.com/2024/01/02/citrix-bleed-security-hacks-impact.

hacked through an exploit of Citrix Bleed, including Boeing, Toyota, and the law firm Allen & Overy.[98]

142. Citrix's decision to publicly announce the vulnerability while simultaneously providing incomplete patching guidance to companies like Comcast was a direct and proximate cause of the Data Breach and provided companies like Comcast a false sense of security that the vulnerability was fixed.

143. Had Citrix revealed the severity of the breach sooner and provided complete patching guidance, the Comcast Data Breach, and many others, may have been mitigated.

G. Comcast Admits It Failed to Protect Plaintiff's PII and Compounded Its Failure by Providing Inadequate Notice to Those Impacted.

144. Comcast announced the breach in a press release on December 18, 2023, and subsequently distributed a "Notice to Customers of Data Security Incident" (the "Notice") to impacted customers. Comcast further distributed supplemental notices to customers.[99] Comcast's first public acknowledgement of the breach thus occurred over two months after Comcast learned of the Citrix Bleed vulnerability and over a month after Comcast concluded that customers' PII had been stolen by cybercriminals exploiting the vulnerability.

145. In the Notice, Comcast admits that cybercriminals were able to exploit the Citrix Bleed vulnerability and acquire customers' PII prior to Comcast's implementation of the vulnerability patch. This is because Comcast's patching policy is inadequate and remains inadequate, and thus, insufficient to prevent another data breach.

---

[98] Dan Goodin, *Xfinity waited to patch critical Citrix Bleed 0-day. Now it's paying the price*, Ars Technica (Dec. 19, 2023 6:14 PM), https://arstechnica.com/security/2023/12/hack-of-unpatched-comcast-servers-results-in-stolen-personal-data-including-passwords/.

[99] *Notice of Data Breach*, Xfinity (January 26, 2024), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/202cb122-b4e6-42fd-b9b5-59e59d44d4fe/c854dc07-5b58-4db8-abb1-2b77342bdc46/SSN_DL%20Notice%20(New)_static%20proof%20r1.pdf.

146. Comcast's Notice, however, failed to disclose how many consumers' PII was breached, leaving consumers to speculate whether it was likely that their own PII has been compromised. Based on a document that Comcast filed with the Maine Attorney General regarding the data breach, however, nearly 36 million former and current Xfinity customers had their PII compromised in the breach.[100]

147. The Notice also demonstrated that Comcast's internal investigation failed to identify which information was stolen for which users:

> On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.[101]

148. The Notice also failed to provide any offer of enhanced identity protection and credit monitoring service and instead contained nothing more than boilerplate language about preventing identity theft and fraud, and simple (and woefully insufficient) suggestions about resetting passwords and setting up two-factor or multi-factor authentication.

H. Defendants Failed to Comply with Industry Standards and Regulatory Guidance Regarding Data Security Practices.

149. Because of the value of PII to hackers and identity thieves, companies that store, maintain, and secure customer PII, such as Comcast, or companies that provide the software and

[100] Office of the Maine AG, *Consumer Information: Privacy, Identity Theft and Data Security Breaches*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (last visited Mar. 20, 2025).
[101] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited Mar. 20, 2025).

hardware used to store, maintain, and secure customer PII, such as Citrix, are particularly vulnerable to cyberattacks.

150. Comcast and Citrix knew their systems were handling, storing, and providing access to large amounts of PII belonging to Plaintiff and other consumers. Just as banks should anticipate that they are attractive targets for thieves due to the large volumes of cash and other valuables that banks routinely store, Comcast and Citrix should have anticipated that their systems would be attractive targets for data thieves.

151. As a result, Comcast and Citrix knew or should have known that failure to safeguard their networks and remote infrastructure could cause foreseeable harm to the customers whose PII was contained in Defendants' systems.

152. Cybersecurity firms and federal agencies have promulgated a series of best practices that should be implemented by companies that handle or facilitate the handling of customer PII, including, at minimum: establishing secure password and authentication procedures for employees; building secure networks by setting up network protection tools like firewalls and constantly monitoring for and patching vulnerabilities; monitoring active and inactive IP addresses, whitelisting software, monitoring Lightweight Directory Access Protocol (LDAP) reconnaissance, monitoring traffic to IP addresses that are on multiple blacklists; encrypting sensitive data using robust encryption algorithms; limiting access to customer data to only relevant staff; and training staff regarding critical points.[102]

[102] *Customer Data Security: Best Practices for Data Privacy*, CDP, https://cdp.com/articles/customer-data-security-best-practices/; *Securing Networks: Best Practices for Cybersecurity in Telecommunications*, Prismecs (Mar. 27, 2024), https://prismecs.com/blog/securing-networks-best-practices-for-cybersecurity-in-telecommunications; NIST, *Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information*, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

153. For example, LDAP reconnaissance occurs when an attacker scans LDAP to gather information that can be used to exploit vulnerabilities for malicious purposes. By scanning LDAP, the attack can collect usernames, email addresses, and other attributes; identify privileged accounts; extract hostnames, IP addresses or device information; and identify accounts with excessive or unintended privileges. There are many tools and techniques that companies can use to identify LDAP reconnaissance and prevent attacks that rely on LDAP reconnaissance.[103]

154. Similarly, threat actors can scan for and utilize inactive IP addresses in a company's system "as a way to infiltrate networks, bypass security measures, and launch attacks."[104] Properly monitoring inactive and active IP addresses on a network can show when an inactive address suddenly becomes active, thus signaling potentially malicious activity on the network.

155. Moreover, scanning tools exist that allow companies to detect when an outbound connection is established to an IP address that is on blacklists, i.e. has been identified as malicious or illegitimate.

156. Comcast and Citrix both recognize these best practices and discuss many of them in their security and privacy policies.

157. Federal and State governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions. For example, Comcast is prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's

[103] *Detecting LDAP Reconnaissance*, Black Lantern Security (June 28, 2021), https://blog.blacklanternsecurity.com/p/detecting-ldap-recoannaissance.
[104] Kinsley, Patrick, *Unused IP Security Addresses: What Are the Risks?*, SparkNav (May 28, 2024), https://sparknav.com/insights/unused-ip-addresses-what-are-the-cybersecurity-risks/.

failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

158. The FTC has issued numerous guides for business outlining reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[105]

159. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[106] The guidelines note businesses should, among other best practices:

a. Protect the personal customer and consumer information that they keep;

b. Properly dispose of personal information that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.[107]

160. The guidelines further recommend that businesses implement an array of specific methods to protect their systems, such as:

a. Using an intrusion detection system to expose a breach as soon as it occurs;

b. Monitoring all incoming traffic for activity indicating someone is attempting to hack the system;

---

[105] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[106] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[107] *See id.*

c. Watching for large amounts of data being transmitted from the system; and

d. Having a response plan ready in the event of a breach.[108]

161. The FTC also recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

162. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations. Indeed, just last year, the FTC brought an enforcement action against telecommunications provider Global Tel*Link Corporation for failing to secure the sensitive data of hundreds of thousands of individuals.[109]

163. Further, the National Institute of Standards in Technology ("NIST") publishes substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data

[108] *Id.*
[109] *FTC Finalizes Order with Global Tel*Link Over Security Failures that Led to Breach of Sensitive Data*, Federal Trade Comm'n (Feb. 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-finalizes-order-global-tellink-over-security-failures-led-breach-sensitive-data.

security controls, network monitoring, breach detection, and incident response.[110] Defendants failed to adhere to the NIST guidance.

164. For example, NIST recommends application whitelisting, which is a security practice that allows only pre-approved and trusted applications to run on a system, blocking any unauthorized or unknown software from executing.[111] This proactive approach is designed to prevent malware, ransomware, and unauthorized software from compromising systems.

165. NIST also emphasizes the "principle of least privilege."[112] This concept includes limiting access to customer data to only relevant staff, usually specific users with specific privileges, is part of the fundamental cybersecurity concept of least privileges, which dictates that users, applications, systems, or processes should be granted only the minimum levels of access necessary to perform their specific tasks. By limiting access rights, organizations can reduce the potential attack surface, mitigate the risk of accidental or intentional misuse of privileges, and enhance their overall system security.

166. Furthermore, NIST recommends terminating sessions in order to ensure maximum efficacy for a newly-installed patch to a vulnerability.[113] This technique "end[s] all active sessions and prevent[s] the attacker form accessing any further information."[114] Had Comcast followed this

---

[110] *Protecting Personal Information: A Guide for Business*, *supra,* note 93 at Table 2, 26-43; *see generally Security and Privacy Controls for Information Systems and Organizations*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last visited Mar. 20, 2025).
[111] *NIST 800-167*, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf (last visited Mar. 20, 2025).
[112] *NIST-SP 800-53*, https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf (last visited Mar. 20, 2025).
[113] *NIST-SP 800-53 (Technique AC-12)*, https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf (last visited Mar. 20, 2025).
[114] Sundaram, Karishma, *Understanding Session Hijacking: How to Keep Your Website Safe* (May 2, 2023), https://www.malcare.com/blog/session-hijacking/.

recommendation and terminated all active sessions after installing the patch, it would have mitigated the Data Breach, even though Comcast only installed the patch after the Data Breach had begun.

167. NIST also recommends the expiration of sessions and periodic re-authentication, suggesting that sessions should be terminated after a period of inactivity (like 15-30 minutes) and users should re-authenticate at least every 12 hours.[115] Had Comcast implemented industry standard session management lifecycle policies, then the hijacked sessions would timeout after inactivity or after a specific number of hours; indeed, Citrix NetScaler Gateway has a session time-out setting that customers like Comcast could deploy.[116] This would have mitigated the Data Breach, if not prevented it altogether.

168. Comcast and Citrix also have obligations created by additional laws, regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to protect Plaintiff's and Class Members' PII from unauthorized access and disclosure.

169. For example, at least twenty-four states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. *See, e.g.*, Cal. Civ. Code § 1798.81.5(b); N.J. Stat. § 56:8-166.12; Ohio Rev. Code Ann. § 1354.03.

170. To provide another example, under the Cable Communications Policy Act, 47 U.S.C. § 551 (the "Cable Act"), cable operators like Comcast must not disclose PII without prior

[115] *NIST-SP 800-63B*, https://pages.nist.gov/800-63-4/sp800-63b.html (last visited Mar. 20, 2025).
[116] *NetScaler: Configure time-out settings*, Cloud Software Group (Jan. 8, 2024), https://docs.netscaler.com/en-us/netscaler-gateway/current-release/vpn-user-config/configure-plugin-connections/configure-time-out-settings.html.

written or electronic consent of the subscriber, and must destroy PII of former subscribers. Cable operators must also provide annual notice of the nature of PII collected; the nature, frequency, and purpose of any disclosure; the period during which information will be maintained; and the times and place at which the subscriber may access such information. Comcast itself acknowledges the obligations imposed on it through the Cable Act at the time of the Data Breach, and stated that a consumer may "enforce the limitations imposed on us by the Cable Act as applicable with respect to your personally identifiable information through a civil lawsuit seeking damages, attorneys' fees, and litigation costs."[117]

171. Comcast and Citrix were, at all times, fully aware of their obligations to comply with these laws, regulations and best practices to protect individuals' PII. Despite their duties, however, Comcast and Citrix failed to fully comply with industry-standard cybersecurity practices, including, but not limited to: setting up proper network segmentation, using secure credential storage rather than storing PII in plain text, engaging in user-activity monitoring, ensuring data-loss prevention, conducting vigilant monitoring for and timely patching vulnerabilities, deploying comprehensive intrusion detection and prevention systems, failing to train and audit employees on basic cybersecurity practices, failing to provide full and complete patching guidance before publicly announcing the vulnerability, failing to adequately test, secure, and monitor the Citrix NetScaler Products, and retaining PII even after a customer terminates Comcast's services.

172. As a result, Comcast and Citrix failed to adequately secure and protect Xfinity customers' PII, allowing Plaintiff's and Class Members' PII to be stolen, disclosed, and misused.

[117] *Our Privacy Policy*, Xfinity (October 28, 2023), https://web.archive.org/web/20231028013943/https://www.xfinity.com/privacy/policy.

I. Comcast Unjustly Benefits from Customers' PII and other Personal Information

173. Plaintiff and Class Members provide their PII to Comcast with the understanding that Comcast will protect their PII.

174. In turn, Comcast benefits from Plaintiff's and Class Members' PII. For example, Comcast uses this PII "to improve [Comcast's] Services, develop new products and services, give recommendations, deliver personalized consumer experiences (including marketing and advertising for our own and others' products and services), investigate theft and other illegal activities, and to ensure a secure online environment."[118]

175. In addition to improving Comcast's Services and developing new products, Comcast directly benefits from Plaintiff's and Class Members' PII by using their PII and other personal information as primary source data to increase revenue in their marketing and advertising divisions.

176. Comcast receives direct monetary revenue at Plaintiff's and Class Members' expense, as Comcast does not protect the very data it profits from.

177. As a result, Plaintiff and Class Members did not receive the benefit of the bargain with Comcast as they did not receive the value of what was promised and are injured as described herein.

J. The Data Breach Put Xfinity Customers at Imminent and Substantial Risk of Fraud, Identity Theft, and Other Cybercrimes.

178. Comcast's and Citrix's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, addresses, zip codes, phone numbers, email addresses, dates of birth, Social Security numbers, and

[118] Comcast, *Comcast Xfinity Privacy Policy* (Sept. 20, 2023), https://web.archive.org/web/20231128085716/https://assets.xfinity.com/assets/dotcom/projects/cix-5055_xfinity-com-welcome-kit-legal/PP_09202023.pdf

usernames and passwords—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

179. Plaintiff's and Class Members' PII from the Data Breach is already circulating on the "dark web." The dark web conceals users' identities and online activity, which makes it difficult for authorities to detect the location or owners of a website when illegally acquired information is disclosed or put up for sale. The pervasive fraud experienced by Plaintiff and Class Members, as set forth above, indicates that Plaintiff's PII is already circulating for sale on the dark web. Additionally, multiple sets of Comcast/Xfinity data were uploaded to a Torrent site called "Fox Store" where cybercriminals sell and purchase stolen PII. This data was uploaded on October 16, 2023, and October 23, 2023—the first day and one week after the Data Breach. Comcast/Xfinity data affiliated with Plaintiff and Class Members were also uploaded to BlackBet in July and September 2024.

180. Plaintiff's stolen PII is circulating on the dark web because it is highly valuable and useful to cybercriminals. Malicious actors can use stolen PII such as a victim's name, date of birth, and last four digits of a Social Security number to, among other things, gain access to consumers' bank accounts, social media, credit card accounts, and other consumer accounts. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain unemployment or other government benefits, obtain government IDs, or create "synthetic identities," whereby a cybercriminal combines real and fake information to create a new "synthetic" identity which makes it even easier to commit fraud.

181. PII is valuable property. Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[119] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the PII it collects about users of its products and services. Indeed, in 2019, the data brokering industry was worth roughly $200 billion.[120] And on the dark web, PII can sell for as much as $363 per record, according to the Infosec Institute.[121]

182. Criminal law also recognizes the value of PII by imposing harsh prison sentences for those who steal PII. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of PII by (1) demanding a ransom or blackmail payment for its destruction, (2) using PII to commit fraud or identity theft, or (3) selling PII to other cybercriminals on the black market and on the dark web.

183. Importantly, even though full Social Security numbers were not involved in the Data Breach for all Class Members, as noted previously, cybercriminals can easily use the information involved in the Data Breach to reverse engineer an individual victim's full Social Security number. Using nothing but an individual's date of birth and state of residence, computer programs can easily predict the first five digits of an individual's Social Security number.[122] Cybercriminals can combine these reverse-engineered digits with the last four digits stolen in the

[119] *Alphabet Inc., Annual Report (Form 10-K)*, SEC, at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.
[120] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[121] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[122] Xeni Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), https://boingboing.net/2009/07/06/reverse-engineering.html.

Data Breach, and then use the victim's full, nine-digit Social Security number to gain access to the victim's accounts and commit more complicated types of fraud.

184. Even if only the last four digits are stolen, however, theft of Social Security numbers creates a particularly alarming situation for Plaintiff and Class Members because those numbers cannot easily be replaced.

185. Plaintiff and Class Members who were Xfinity Mobile or NOW Mobile customers specifically also face an imminent risk of falling victim to "SIM-swap" fraud. A SIM swap is a scheme whereby a hacker gains control of a victim's mobile phone number and service in order to intercept communications intended for the victim, including text messages that a victim's customer, financial, and medical accounts may use to verify the victim's identity for login purposes. Following a fraudulent SIM swap, the legitimate subscriber (now victim)'s phone loses connection to the wireless network, meaning they cannot use the wireless network to call, text, or use the internet, and they are inhibited in their attempts to warn their wireless carrier of the fraud. All phone calls and text messages that would normally have gone to the victim's phone now go to the imposter's phone. Hackers can thus easily use the victim's phone number as a key to access and take over the victim's other digital accounts, such as email, file storage, and financial accounts.

186. In addition to the risk of a SIM swap faced by Xfinity Mobile and NOW Mobile customers, all Xfinity customers impacted by the Data Breach also face a substantial and imminent risk of "port-out" fraud discussed previously, whereby cybercriminals hijack a victim's phone number using the victim's name, address, birth date, passwords, and the last four digits of his or her Social Security number.

187. Once cybercriminals start committing fraud and other identity theft-related crimes using a victim's PII, the disruption to the victim's life can be catastrophic. A study by the Identity

Theft Resource Center ("ITRC") found that, among individuals who experienced fraudulent use of their PII, nearly all of them had experienced some form of costs or other harm in their lives, including having to borrow money, being forced out of their home or residence, and being unable to care for their family.[123] Indeed, as the U.S. Government Accountability Office ("GAO") found in a 2007 report, victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[124]

188. Further, although the theft of PII creates an imminent risk of becoming a victim of identity theft and fraud, malicious actors often wait months or years to use the PII obtained in data breaches. GAO determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[125] During this delay, victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. Plaintiff and many of the Class Members are younger, and Plaintiff must vigilantly monitor his financial accounts for many years to come.

189. Cybercriminals will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact

---

[123] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

[124] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, U.S. Gov't Accountability Office (June 2007), https://www.gao.gov/assets/270/262899.pdf.

[125] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm.

that the Data Breach centralizes the PII and identifies the victims as Xfinity's current and former customers materially increases the risk to Plaintiff and the Class.

190. Plaintiff and Class Members are particularly at risk of additional data breaches because part of the PII stolen in the Data Breach involved their usernames and passwords, which makes it far more likely that Plaintiff and Class Members will be victims of a future "credential stuffing" attack.

191. Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts on other systems through large-scale automated login requests that test whether the user's stolen credentials are *also* used for other systems and accounts. Credential stuffing was behind several notable recent data breaches, including 23andMe[126] and Roku.[127] Even if cybercriminals use Plaintiff's and Class Members' data to commit fraud and identity theft immediately, there is often a lag between when a person suffers harm due to theft of their PII and when they *discover* that harm. The substantial and imminent risk that Plaintiff currently face therefore will not decrease over the next several months and years; on average, it takes approximately three months for a consumer to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[128] Plaintiff will

[126] Mack DeGeurin, *Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move*, The Guardian (Feb. 15, 2024), https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response.
[127] Jeffrey Burt, *Roku: Credential Stuffing Attacks Affect 591,000 Accounts*, Security Boulevard (Apr. 15, 2024), https://securityboulevard.com/2024/04/roku-credential-stuffing-attacks-affect-591000-accounts/.
[128] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII is not used in malicious ways to harm them.

192. Beyond all of the injuries described, events like the Data Breach also have a deep psychological impact on their victims:

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you […].[129]

PLAINTIFF'S AND CLASS MEMBERS' INJURIES AND DAMAGES

193. Plaintiff and Class Members are current and former customers of Comcast, including current and former subscribers to Comcast's Xfinity Internet, TV/Cable, Phone/Voice, Home Security, and/or Xfinity Mobile services. Plaintiff and Class Members were required to provide PII to Comcast in exchange for access to these services, which Comcast had a duty to secure and safeguard.

194. As a direct and proximate result of Citrix's and Comcast's failure to institute adequate data security measures, Plaintiff and Class Members were injured and incurred damages when third-party cybercriminals breached Citrix's products and Comcast's systems and stole Plaintiff's and Class Members' PII.

195. Indeed, Plaintiff's and Class Members' PII was compromised as a direct and proximate result of the Data Breach. While Comcast knew of the Citrix Bleed vulnerability as early as October 10, 2023, Comcast waited an unreasonable amount of time to patch the vulnerability on allegedly all affected systems, leaving Plaintiff's PII vulnerable to cybercriminals. Moreover, Plaintiff did not start receiving the Notice until around December 20, 2023, at the

[129] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

earliest—over two months after the vulnerability was announced and the Data Breach occurred. Like Plaintiff, Class Members' PII was also compromised as a direct and proximate result of the Data Breach.

196. The harm faced by Plaintiff and Class Members is substantial and imminent, as unauthorized cybercriminals now have possession of their information, available for their use however and whenever they see fit, including posting or selling that information on the dark web. Defendants acknowledge that the risk borne by Plaintiff and Class Members is a real one, as evidenced by the Notice sent by Comcast to Plaintiff, which advises Plaintiff to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

197. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been injured in many other ways.

198. First, Plaintiff and Class Members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff in the near future. This harm can be quantified by putting Plaintiff and the Class in the position they would have been in but for the Data Breach, including by quantifying the cost of high-quality monitoring for Plaintiff and the Class.

199. Second, as noted previously, there is often a lag between cybercriminals' acquisition of PII and use of that information to commit fraud, identity theft, phishing, and other schemes. As a direct and proximate result of Comcast's and Citrix's conduct, Plaintiff and Class Members must incur and continue to incur out-of-pocket costs for protective measures such as on-

going high quality credit monitoring and additional costs for credit report fees, and similar costs directly related to the Data Breach, for years to come.

200. Third, and relatedly, Plaintiff and Class Members have and will suffer ascertainable losses in the form of out-of-pocket expenses and the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

201. Fourth, Plaintiff and Class Members have lost the value of their PII because the information is a valuable commodity. PII is a valuable commodity on the black market, and one study of PII vendors on the dark web estimated that a limited group of vendors received more than $140 million from the sale of stolen PII in just eight months.[130] Indeed, PII is a valuable asset even among legal companies and entities,[131] with "Big Data" corporations like Alphabet, Inc. earning hundreds of *billions* of dollars annually in recent years by leveraging PII that they collect.[132] Some companies are now explicitly offering consumers money in exchange for a non-exclusive license to use their personal information, up to nearly $50 per month.[133] Thus, PII has considerable market value that is diminished when it is compromised. Further, because Defendants allowed unauthorized access to Plaintiff's and Class Members' PII, Plaintiff and Class Members were deprived of the value of such access.

202. Fifth, Plaintiff and Class Members are, at the very least, entitled to nominal damages for Comcast's and Citrix's violations as discussed herein. As a result of Comcast's and Citrix's failure to safeguard Plaintiff's and Class Members' PII, Plaintiff and Class Members are

---

[130] Christian J. Howell & David Maimon, *Darknet markets generate millions in revenue selling stolen personal data, supply chain study finds*, The Conversation (Dec. 2, 2022, 8:42 AM), https://theconversation.com/darknet-markets-generate-millions-in-revenue-selling-stolen-personal-data-supply-chain-study-finds-193506.

[131] *See, e.g.*, John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[132] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

[133] Tatum Hunter, *These companies will pay you for your data. Is it a good deal?*, Washington Post (Feb. 6, 2023, 6:00 AM), https://www.washingtonpost.com/technology/2023/02/06/consumers-paid-money-data/.

forced to live with the knowledge that their PII—which contains private and personal details of their life—has likely been disclosed or made available for sale to the entire world online, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiff and Class Members of their fundamental right to privacy.

203. Sixth, Plaintiff and Class Members are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below.

204. Seventh, Comcast and Citrix were unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Among other things, Comcast continues to benefit and profit from their PII while its value to Plaintiff and Class Members has been diminished.

205. Eighth, Plaintiff and Class Members are also entitled to actual damages measured by the difference in the value of Comcast's services promised to them and the value of what Plaintiff and Class Members received from Comcast.

206. Ninth, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of Comcast is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiff's and Class Members' data is not accessible online and that access to such data is limited and secured.

207. Finally, Plaintiff and Class Members are entitled to equitable relief as there is no adequate remedy at law for certain prospective harms. Comcast and Citrix have not yet implemented adequate cybersecurity measures and cyber policies to prevent a future data breach. For example, Comcast's patching policies, session management, information security, access controls, among other things, remain inadequate. And Comcast continues to misrepresent its data security practices to the Class and prospective customers (i.e., the public) through its privacy

policy and otherwise. Nor have they provided adequate notice to all Class Members. Similarly, Citrix still fails to adequately test and monitor its NetScaler Products, which still provide access to Plaintiff's and Class Members' PII. Thus, equitable relief here preventing Defendants from continuing their actions would prevent future, prospective harm

CLASS ALLEGATIONS

208. Plaintiff brings this Class Action on behalf of himself and all other similarly situated individuals Rules 1702, 1708 and 1709 of the Pennsylvania Rules of Civil Procedure.

209. Plaintiff seeks to represent a 49-State Class and Cable Act Subclass to be defined as follows:

> **49-State Class**: All natural persons residing in the United States, excluding California, whose Personally Identifiable Information was compromised as a result of the Data Breach.
>
> **Cable Act Subclass**: All natural persons residing in the United States, excluding California, whose Personally Identifiable Information was compromised as a result of the Data Breach, and who received Xfinity Residential Services (including Xfinity Cable Television, Xfinity TV, Xfinity Internet, and/or Xfinity Voice).

210. Excluded from the Class and Subclass are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

211. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for

class certification as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

212. **Numerosity – Pennsylvania Rule of Civil Procedure 1702(1):** The members of the Class (and Subclass) are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the class consists of millions of persons whose data was compromised in the Data Breach who can be identified by reviewing the PII exfiltrated from Comcast's databases. Based upon public filings, the current number of people impacted is approximately 36 million.

213. **Commonality – Pennsylvania Rule of Civil Procedure 1702(2):** There are questions of law and fact common to Plaintiff and Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Comcast unlawfully used, maintained, or disclosed Plaintiff's and the Class Members' PII;

b. Whether Comcast and Citrix failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

c. Whether Comcast and Citrix truthfully represented the nature of their security systems, including their vulnerability to hackers;

d. Whether Comcast's and Citrix's data security protocols prior to and during the Data Breach complied with applicable data security laws and regulations;

e. Whether Comcast's and Citrix's data security protocols prior to and during the Data Breach were consistent with industry standards;

f. Whether Citrix's remedial patching guidance was complete;

g. Whether Comcast and Citrix each owed a duty to Class Members to safeguard their PII;

h. Whether Comcast and Citrix breached their duties to Class Members to safeguard their PII;

i. Whether cyberhackers obtained, sold, copied, stored or released Class Members' PII;

j. Whether Comcast and Citrix knew or should have known that their data security programs and monitoring processes were deficient;

k. Whether and when Comcast and Citrix actually learned of the Data Breach;

l. Whether Comcast adequately, promptly, and accurately informed Plaintiff and Class Members that their PII was compromised;

m. Whether Comcast violated the law by failing to adequately, promptly, and accurately inform Plaintiff and Class Members that their PII was compromised;

n. Whether the Class Members suffered legally cognizable damages as a result of Comcast's and Citrix's misconduct; and

o. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

214. **Typicality – Pennsylvania Rule of Civil Procedure 1702(3):** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on

the same legal theories and arise from the same unlawful and willful conduct. Plaintiff's claims are typical of those of the Class Members because Plaintiff's PII, like that of every class member, was compromised in the Data Breach.

215. **Adequacy of Representation – Pennsylvania Rule of Civil Procedure 1702(4) and 1709:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members, including from those states and jurisdictions where he does not reside, and has no interests antagonistic to the Class Members. The claims of Plaintiff and the Class Members are substantially identical, as explained above. In addition, Plaintiff's counsel are competent and experienced in the prosecution of data breach class action litigation.

216. **Predominance – Pennsylvania Rule of Civil Procedure 1708(a)(1):** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. Comcast and Citrix have each engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and the Class Members' data at issue here was stored by Comcast using Citrix appliances and was accessed during the Data Breach. The common issues arising from Comcast's and Citrix's respective conduct affecting Class Members, as described *supra*, thus predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

217. **Manageability – Pennsylvania Rule of Civil Procedure 1708(a)(2):** While the exact number of Class Members is unknown to Plaintiff at this time, based on information and

belief, the class consists of millions of persons whose data was compromised in the Data Breach who can be identified by reviewing the PII exfiltrated from Comcast's databases. Based upon public filings, the current number of people impacted is approximately 36 million. The claims of Plaintiff and these Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

218. **Risk of Inconsistent, Varying or Prejudicial Adjudications – Pennsylvania Rule of Civil Procedure 1708(a)(3):** If the claims of Plaintiff and the members of the Class were tried separately, Defendant may be confronted with incompatible standards of conduct and divergent court decisions. Furthermore, if the claims of Plaintiff and the members of the Class were tried individually, adjudications with respect to individual Class members and the propriety of their claims could be dispositive on the interests of other members of the Class not party to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

219. **Litigation Already Commenced – Pennsylvania Rule of Civil Procedure 1708(a)(4)**: To Plaintiff's knowledge, no other pending case in Pennsylvania courts seeks to represent a class of individuals impacted by the conduct alleged in this Complaint. As noted in a prior footnote, there is an ongoing consolidated federal action arising from the conduct alleged in this Complaint. *See Hasson v. Comcast Cable Commc'ns LLC et al.*, No. 2:23-cv-5039 (E.D. Pa.). However, Defendants moved to dismiss that litigation, arguing that that the plaintiffs lack Article III standing for claims arising from the Data Breach and the federal courts lack jurisdiction over

such claims. Plaintiff brings this action in this Court to protect the interests of the class of customers impacted by the Data Breach.

220. **The Appropriateness of the Forum – Pennsylvania Rule of Civil Procedure 1708(a)(5):** This is the most appropriate forum to concentrate the litigation because the Defendants conduct business in this County, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this County, and Plaintiff's alleged injuries occurred in this County.

221. **The Class Members' Claims Support Certification – Pennsylvania Rule of Civil Procedure 1708(a)(6) and (7)**. Given the potentially low amount recoverable by each Class member, the expenses of individual litigation are insufficient to support or justify individual suits. Furthermore, the damages that may be recovered by the Class will not be so small such that class certification is unjustified.

222. **The General Applicability of Defendants' Conduct – Pennsylvania Rule of Civil Procedure 1708(b)(2).** Defendants' failure to secure PII is generally applicable to the Classes as a whole, making equitable and declaratory relief appropriate with respect to each Class Member.

CAUSES OF ACTION

223. Plaintiff brings these causes of action on behalf of the 49-State Class and Cable Act Subclass, as defined herein. The application of one specific state's laws to any cause of action is premature at this juncture, without the benefit of discovery, as Comcast maintained servers and Citrix NetScaler appliances in several states, and Xfinity customers exist across the United States.

FIRST CAUSE OF ACTION
CABLE COMMUNICATIONS POLICY ACT
47 U.S.C. §§ 521 et seq.
(On behalf of Plaintiff and the 49-State Class, or alternatively, on behalf of Plaintiff and the Cable Act Subclass, against Comcast only)

224. Plaintiff restates and realleges all foregoing factual allegations as if fully set forth herein.

225. The Cable Communications Policy Act provides in relevant part that "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator." 47 U.S.C § 551(c).

226. The Cable Communications Policy Act further provides that a "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court." 47 U.S.C § 551(f)(1).

227. Comcast is a cable operator as it "provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system," or "otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system." 47 U.S.C. § 522(5).

228. Comcast's provision of Xfinity TV and cable services to Plaintiff and Class Members qualifies as "cable services" as defined by the Cable Communications Policy Act because such services include "the one-way transmission to subscribers of video programming or other programming service and subscriber interaction which is required for the selection or use of the video programming or other programing service." 47. U.S.C. § 522 (6).

229. Comcast's provision of Internet service to Plaintiff and Class Members separately qualifies as an "other service" as defined by the Cable Communications Policy Act because such

Internet service is a "wire or radio communication[] service provided using any of the facilities of a cable operator that are used in the provision of cable service." 47 U.S.C § 551(a)(2).

230. Comcast's provision of Xfinity Voice service to Plaintiff and Class Members also separately qualifies as an "other service" as defined by the Cable Communications Policy Act because such Voice service is a "wire or radio communication[] service provided using any of the facilities of a cable operator that are used in the provision of cable service." 47 U.S.C § 551(a)(2).

231. Plaintiff's and Class Members' PII is "personally identifiable information" within the meaning of 47 U.S.C § 551.

232. Plaintiff and Class Members are "subscribers" of Comcast's "cable services" and "other services" within the meaning of 47 U.S.C. § 551 because they have paid for and/or purchased cable/television service, internet service, and/or mobile service from Comcast.

233. At all relevant times hereto, pursuant to 47 U.S.C. § 551, Comcast was required to take such actions as necessary to prevent unauthorized access to Plaintiff's and Class Members' PII by a person other than the subscriber or cable operator.

234. Comcast violated 47 U.S.C § 551(c) by failing to prevent unauthorized access to Plaintiff's and Class Members' PII by unauthorized third parties. Comcast violated 47 U.S.C §§ 551(c) and (e) through the following errors and omissions, among others described herein, that allowed the Data Breach to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and

procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII; (i) failing to timely patch known vulnerabilities to its computer systems or networks; and (j) failing to destroy PII no longer necessary for the purpose for which it was collected, including the PII of former customers who no longer access their terminated Comcast account. Comcast also violated 47 U.S.C. § 551(a) by not providing notice that clearly and conspicuously informed Plaintiff and Class Members that Comcast would disclosure their PII as it did during the Data Breach and that Comcast stores their data for an indefinite amount of time.

235. As a direct and proximate result of Comcast's violation of 47 U.S.C § 551 (a), (c), (e), Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent

charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Comcast with the mutual understanding that Comcast would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Comcast's possession and is subject to further breaches so long as Comcast fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

236. As a direct and proximate result of Comcast's violation of the Cable Communications Policy Act, Plaintiff and Class Members seek statutory damages of at least $1,300 per subscriber per violation or actual damages (the statute awards damages of $100 per day or $1,000, whichever is greater, and Comcast's violation lasted from approximately October 10–

23, 2023), as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

SECOND CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiff and the 49-State Class against Comcast only)

237. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

238. Comcast required Plaintiff and Class Members to submit their sensitive PII in order to obtain or apply for its products and/or services.

239. Comcast owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Comcast's security systems to ensure that Plaintiff's and Class Members' PII in Comcast's possession was adequately protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generating by its own security systems, regarding instructions to its networks or systems; (d) maintaining security measures consistent with industry standards; (e) exercising appropriate discretion in selecting third-party vendors with whom it makes Plaintiff's and Class Members' PII available; (f) exercising appropriate control over Citrix's data security practices, and (g) timely rectifying known vulnerabilities its networks or systems.

240. Comcast's duty to use reasonable care arose from several sources, including but not limited to those described below.

241. Comcast has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Comcast. By receiving, maintaining, and handling valuable PII that is routinely targeted by criminals for unauthorized access and use for nefarious purposes, Comcast was obligated to act with reasonable care to protect against these foreseeable threats.

242. Comcast also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. Comcast's conduct included its failure to adequately restrict access to its computer networks and systems that held Plaintiff's and Class Members' PII, as Comcast knew it was more than likely than not Plaintiff and Class Members would be harmed if it allowed such a breach of its computer networks and systems.

243. Comcast's duty also arose as a result of the special relationship that existed between Comcast, on the one hand, and Plaintiff and Class Members on the other hand. The special relationship arose because Plaintiff and Class Members entrusted Comcast with their PII as part of the applications for and/or purchase and signing up for the products Comcast offers as a major telecommunications company. Comcast alone could have ensured that its security systems were sufficient to prevent or minimize the Data Breach.

244. Comcast's duty also arose from Comcast's unique position as one of the largest telecommunications companies in the United States. As a telecommunications company, Comcast holds itself out as a protector of consumer data and thereby assumes a duty to reasonably protect the PII that it was entrusted by Plaintiff and Class Members. Comcast has stated that "[w]e know you rely on us to stay connected to the people and things you care about most and your privacy is essential when you use our products and services. That's why we're always working to keep your

personal information secure and put you in control of it."[134] Because of its role as one of the largest telecommunications companies in the U.S., Comcast was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

245. Comcast admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect Plaintiff's and Class Members' PII.

246. Further, Comcast's duty arose from various statutes requiring Comcast to implement reasonable data security measures, including but not limited to: Section 5 of the FTC Act. For example, Section 5 of the FTC Act required Comcast to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Comcast's duty to Plaintiff and the Class. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Comcast for failing to use reasonable measures to protect highly sensitive data. Therefore, Comcast was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Comcast's duties to adequately protect sensitive information.

247. Comcast is subject to an "independent duty," untethered to any contract between Comcast and Plaintiff and Comcast and Class Members. The sources of Comcast's duty are identified above.

248. Comcast breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Comcast breached its duties through

[134] *Privacy*, Xfinity, https://www.xfinity.com/privacy (last visited Mar. 20, 2025).

some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII; and (i) failing to timely patch known vulnerabilities to its computer systems or networks.

249. But for Comcast's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

250. Comcast's failure to implement adequate security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conductive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

251. Plaintiff and Class Members were the foreseeable victims of Comcast's inadequate data security measures, and it was also foreseeable that Comcast's failure to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members as described in this Consolidated Class Action Complaint.

252. As a direct and proximate result of Comcast's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Comcast with the mutual understanding that Comcast would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Comcast's possession and is subject to further breaches so long as Comcast fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

253. As a direct and proximate result of Comcast's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the 49-State Class against Comcast only)

254. Plaintiff restates and realleges all foregoing factual allegations as if fully set forth herein.

255. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Comcast for failing to use reasonable measures to protect consumer PII. Various FTC publications and orders also form the basis of Comcast's duty.

256. Comcast violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumer PII and not complying with the industry standards. Comcast's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the

foreseeable consequences of a data breach involving a company as large as Comcast, including the damages that would result to Plaintiff and Class Members.

257. Comcast's violation of Section 5 of the FTC Act constitutes negligence *per se*.

258. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

259. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

260. Comcast also violated the Cable Communications Policy Act as described in Count I above.

261. Comcast's violation of the Cable Communications Policy Act also constitutes negligence *per se*.

262. Plaintiff and Class Members are subscribers of "cable services" and "other services" within the class of persons the Cable Communications Policy Act was intended to protect. And the harm that has occurred is the type of harm that the Cable Communications Policy Act was intended to guard against. Indeed, the Cable Communications Policy Act was intended to protect subscribers from the harm caused by the unauthorized disclosure and unlawful retention of subscribers' PII—the same harms alleged herein.

263. Comcast breached its duties to Plaintiff and Class Members under Section 5 of the FTC Act and the Cable Communications Policy Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

264. Plaintiff and Class Members were foreseeable victims of Comcast's violations of Section 5 of the FTC Act and the Cable Communications Policy Act. Comcast also knew or should have known that its failure to implement reasonable data security measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

265. But for Comcast's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been compromised by unauthorized third parties.

266. As a direct and proximate result of Comcast's negligence *per se*, Plaintiff and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiff and the 49-State Class against Comcast only)

267. Plaintiff restates and realleges all foregoing paragraphs as if fully set forth herein.

268. Comcast's Privacy Policy[135] is an agreement between Comcast and individuals who provided their PII to Comcast, including Plaintiff and Class Members.

269. Comcast's Privacy Policy states that "it applies to the information we collect when you use or interact with the business entities, products, services, networks, and platforms, including our websites, mobile apps, and other services and devices where this policy is referenced. These may include Xfinity-branded services, Comcast-branded Services, Xumo-branded Services, and other products and services we deliver."[136]

[135] Citations throughout Count 3 are to *Privacy Policy*, Xfinity (effective Sept. 20, 2023), https://web.archive.org/web/20231004141125/https://www.xfinity.com/privacy/policy/.
[136] Examples of when the Privacy Policy applies include: "Xfinity® TV and Streaming, Xfinity Internet, xFi and Xfinity Advanced Security, Xfinity Voice, Xfinity Stream app, Xfinity WiFi service, Xfinity Home, Xfinity Mobile, Xfinity Flex, Comcast Business Services, Effectv, Xumo, Xumo TV, Xumo Play."

270. Comcast's Privacy Policy stated at the time of the Data Breach that Comcast "follow[s] industry-standard practices to secure the information [it] collect[s] to prevent the unauthorized access, use, or disclosure of any personal information [Comcast] collect[s] and maintain[s]."

271. Comcast further promised at the time of the Data Brech that it would only share Plaintiff's and Class Members' data under certain enumerated circumstances, which include: "The Comcast family of business;" "Account owners and other authorized users;" "Service providers," such as billing and collection providers, accounting, auditing and tax providers, and marketing, advertising, and sales programs; and "Third parties," such as online advertising partners, consumer reporting agencies, and directory services. None of the enumerated circumstances involve sharing Plaintiff's or Class Members' PII with unauthorized third parties.

272. Comcast emphasized in its Privacy Policy at the time of the Data Breach that "we take our responsibility of safeguarding your personal information seriously" and further referenced the "Xfinity Privacy Center," which stated that "[w]e know you rely on us to stay connected to the people and things you care about most and your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it."[137]

273. Plaintiff and Class Members on the one side, and Comcast on the other, formed a contract when Plaintiff and Class Members obtained products or services from Comcast, or otherwise provided PII to Comcast subject to its Privacy Policy.

[137] https://web.archive.org/web/20231028014023/https://www.xfinity.com/privacy (captured Oct. 28, 2023).

274. Plaintiff and Class Members fully performed their obligations under the contracts with Comcast.

275. Comcast breached its agreements with Plaintiff and Class Members by failing to protect their PII. Specifically, Comcast: (1) failed to take reasonable steps to secure its computer networks and systems to protect PII; and (2) disclosed Plaintiff's and Class Members' PII to unauthorized third parties, in violation of the agreement.

276. As a direct and proximate result of Comcast's breach of contract. Plaintiff and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Such injuries include: lost benefit of their bargains, overcharges for services or products, and those described herein.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the 49-State Class against Comcast only)

277. Plaintiff restates and realleges all foregoing factual allegations, except those under Count 4, as if fully set forth herein.

278. Plaintiff brings this claim in the alternative to his breach of express contract claim.

279. Plaintiff and Class Members entered into implied contracts with Comcast when they obtained products or services from Comcast, or otherwise provided PII to Comcast. Indeed, Plaintiff and Class Members were required to provide their PII to Comcast as a condition of using Comcast's products and/or services.

280. In doing so, Plaintiff and Class Members entered into implied contracts with Comcast by which Defendant agreed to safeguard and protect such PII and keep such PII secure and confidential.

281. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Comcast's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and to timely notify them of a data breach. Plaintiff and Class Members further reasonably believed and expected that Comcast would use part of the monies paid to Comcast under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security measures.

282. Indeed, implicit in these exchanges was a promise by Comcast to ensure the PII of Plaintiff and Class Members in its possession would be used to provide the agreed-upon services and that Comcast would take adequate measures to protect Plaintiff's and Class Members' PII.

283. It is clear by these exchanges that the Parties intended to enter into implied agreements supported by mutual assent. Plaintiff and Class Members would not have disclosed their PII to Comcast but for the prospect of Comcast's promise of services and/or products. Conversely, Comcast presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members with products and services.

284. Plaintiff and Class Members would not have provided their PII to Comcast or would have paid less for Comcast services or products in the absence of the implied contract between them and Comcast as the safeguarding of Plaintiff's and Class Members' PII was critical to realize the intent of the parties.

285. Plaintiff and Class Members fully performed their obligations under their implied contracts with Comcast.

286. Comcast breached its implied contracts with Plaintiff and Class Members by failing to protect their PII. Specifically, Comcast: (1) failed to take reasonable steps to secure its computer

networks and systems to protect PII; and (2) disclosed Plaintiff's and Class Members' PII to unauthorized third parties, in violation of the agreement.

287. As a direct and proximate result of Comcast's breach of implied contract. Plaintiff and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Such injuries include: lost benefit of their bargains, overcharges for services or products, and those described above herein.

SIXTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiff and the 49-State Class against Comcast only)

288. Plaintiff restates and realleges all foregoing factual allegations, except those under Counts 4 and 5, as if fully set forth herein.

289. Plaintiff brings this claim in the alternative to their breach of express and breach of implied contract claims.

290. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Comcast and that was ultimately compromised in the Data Breach.

291. By engaging in the conduct described in this Complaint, Comcast has knowingly obtained and derived benefits from Plaintiff and Class Members at Plaintiff's and Class Members' expense, namely the profits gained from payment and provision of PII in exchange for the use of Comcast's services, such that it would be inequitable and unjust for Defendant to retain.

292. Comcast also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended on Comcast maintaining the privacy and confidentiality of that PII.

293. But for Comcast's willingness and commitment to maintaining Plaintiff's and Class Members' PII, that PII would not have been transferred to and entrusted with Comcast.

294. Comcast admits that it uses the PII it collects for, among other things, advertising and marketing for its own and others' products and services, to improve its services, "develop new products and services, give recommendations, deliver personalized consumer experiences."[138]

295. Because of its use of Plaintiff's and Class Members' PII, Comcast has sold more services and products than it otherwise would have. Comcast was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

296. Further, by engaging in the acts and failures to act described in this Consolidated Amended Complaint, Comcast has been knowingly enriched by the savings in costs that should have been reasonably expensed to protect the PII of Plaintiff and the Class. Comcast knew or should have known that theft of consumer PII could happen, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of its consumers' PII.

297. Comcast's failure to direct profits derived from Plaintiff's and Class Members' payments for services toward safeguarding Plaintiff's and Class Members' PII constitutes the inequitable retention of a benefit without payment for its value.

298. Comcast will be unjustly enriched if it is permitted to retain the benefits derived after the theft of Plaintiff's and Class Members' PII.

[138] *Privacy Policy*, Xfinity (effective Sept. 20, 2023), https://web.archive.org/web/20231004141125/https://www.xfinity.com/privacy/policy/.

299. It is inequitable, unfair, and unjust for Comcast to retain these wrongfully obtained benefits. Comcast's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience

300. The benefit conferred upon, received, and enjoyed by Comcast was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Comcast to retain the benefit.

301. Comcast's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

302. Plaintiff and Class Members have no adequate remedy at law.

303. Comcast is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on Comcast as a result of its wrongful conduct, including specifically: the value to Comcast of the PII that was stolen in the Data Breach; the profits Comcast received and is receiving from the use of that information; the amounts that Comcast overcharged Plaintiff and Class Members for use of Comcast's products and services; and the amounts that Comcast should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

SEVENTH CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiff and the 49-State Class against Citrix only)

304. Plaintiff repeats and realleges the preceding factual allegations set forth in paragraphs 1 to 223 as if fully alleged herein.

305. Plaintiff and Class Members were required to submit their sensitive PII to Comcast in order to obtain or apply for its products and/or services. To collect, manage, and store the data that Plaintiff and Class Members entrusted to Comcast, Comcast utilized allegedly secure appliances/software produced and maintained by Citrix.

306. Citrix, as an entity that helps to store and maintain Plaintiff's and Class Members' PII, owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in securing, safeguarding, and protecting their PII from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Citrix's appliances and security systems to ensure that Plaintiff's and Class Members' PII in Citrix's clients' possession, including Comcast's possession, was adequately protected; (b) implementing processes that would detect vulnerabilities or breaches of its systems in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own systems and those publicized by third-parties, regarding its networks or systems; (d) maintaining security measures consistent with industry standards; (e) timely rectifying known vulnerabilities its networks or systems; and (f) timely releasing adequate guidance to its customers regarding known vulnerabilities in its networks or systems.

307. Citrix's duty to use reasonable care arose from several sources, including but not limited to those described below.

308. Citrix has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Citrix. By helping its customers maintain and handle valuable PII that is routinely targeted by criminals for unauthorized access and use for nefarious

purposes, Citrix was obligated to act with reasonable care to protect against these foreseeable threats.

309. Citrix also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. Citrix's conduct included its failure to adequately test its products, networks, and systems that stored and managed Plaintiff's and Class Members' PII, as Citrix knew it was more than likely than not Plaintiff and Class Members would be harmed if it failed to timely disclose and patch a vulnerability in its products used by Comcast.

310. Citrix also owed a common law duty because its affirmative conduct created a foreseeable risk of harm to Plaintiff and Class Members. Citrix's affirmative act in announcing the Citrix Bleed vulnerability while simultaneously releasing incomplete patching guidance (and ultimately not releasing full and complete guidance until nearly two weeks later) gave rise to a duty to Plaintiff and Class Members, as Citrix knew it acted without exercising reasonable care and that Plaintiff and Class Members would likely be harmed as a result of its conduct.

311. Citrix's duty also arose, indirectly, as a result of the special relationship that existed between Comcast and its customers, including Plaintiff and Class Members. The special relationship arose because Plaintiff and Class Members entrusted Comcast with their PII as part of the applications for and/or purchase and signing up for the products Comcast offers as a major telecommunications company, which Comcast in turn then entrusted to software and products produced and managed by Citrix. Citrix alone could have ensured that its own security systems were sufficient to prevent or minimize the Data Breach.

312. Citrix's duty also arose from Citrix's unique position as one of the largest cloud computing and virtualization companies in the United States. As a large, multinational technology company, Citrix holds itself out as a protector of data collected by its customers, including

Comcast, and thereby assumes a duty to reasonably protect the PII that Plaintiff and Class Members entrusted to Comcast and, by extension, Citrix. Citrix has stated that: "For almost 30 years, our customers have trusted our ability to handle their data with care and respect. That's why organizations from the most highly regulated sectors rely on us to protect their most sensitive information wherever work happens."[139] Indeed, because of its role as one of the largest office technology companies in the U.S., Citrix was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

313. Further, Citrix's duty arose from various statutes requiring Citrix to implement and utilize reasonable data security measures, including but not limited to Section 5 of the FTC Act. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Citrix of failing to use reasonable measures to protect highly sensitive data. Therefore, Citrix was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein, as well as other federal and state laws and regulations, thus form the basis of Citrix's duties to adequately protect sensitive information.

314. Citrix is subject to an "independent duty," untethered to any contract that may exist between Citrix and Plaintiff and Citrix and Class Members. The sources of Citrix's duty are identified above.

315. Citrix breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties to exploit

[139] *Citrix Trust Center: Privacy & Certifications*, Citrix, https://www.citrix.com/about/trust-center/privacy-compliance.html (last visited Mar. 20, 2025).

the Citrix Bleed vulnerability are unclear at this time, on information and belief, Citrix breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of its NetScaler products and other products, which resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to adequately engage in penetration and vulnerability testing to assess and mitigate these risks; (d) failing to design and implement safeguards to control these risks; (e) failing to adequately test and monitor the effectiveness of the safeguards' controls, systems, and procedures; (f) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (g) failing to detect the Citrix Bleed vulnerability and exploitation thereof at the time the exploitation began or within a reasonable time thereafter; (h) failing to follow its own privacy policies and practices published to its customers; (i) failing to adequately train and supervise employees regarding the risk inherent to its customers' use of its products to collect, manage, and store sensitive PII; and (j) failing to timely identify and patch known vulnerabilities in its products, systems, or networks.

316. But for Citrix's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

317. Citrix's failure to implement adequate security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conductive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

318. Plaintiff and Class Members were the foreseeable victims of Citrix's inadequate data security measures, and it was also foreseeable that Citrix's failure to protect Plaintiff's and

Class Members' PII would result in injury to Plaintiff and Class Members as described in this Consolidated Class Action Complaint.

319. As a direct and proximate result of Citrix's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Citrix with the mutual understanding that Citrix would

safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in the possession of Citrix's customers, namely Comcast, and is subject to further breaches so long as Citrix fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

320. As a direct and proximate result of Citrix's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

EIGHTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the 49-State Class against Citrix only)

321. Plaintiff repeats and realleges the preceding factual allegations set forth in paragraphs 1 to 223 as if fully alleged herein.

322. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Citrix for failing to use reasonable measures to protect consumer PII. Various FTC publications and orders also form the basis of Citrix's duty.

323. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumer PII and not complying with the industry standards. Citrix's conduct was

particularly unreasonable given the nature and amount of PII that Citrix's customers, such as Comcast, obtained and stored, and the foreseeable consequences of a data breach involving Citrix's widely used NetScaler products, including the damages that would result to Plaintiff and Class Members.

324. Citrix's violation of Section 5 of the FTC Act constitutes negligence *per se*.

325. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

326. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

327. Citrix breached its duties to Plaintiff and Class Members under Section 5 of the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

328. Plaintiff and Class Members were foreseeable victims of Citrix's violations of Section 5 of the FTC Act. Citrix also knew or should have known that its failure to implement reasonable data security measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

329. But for Citrix's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been compromised by unauthorized third parties.

330. As a direct and proximate result of Citrix's negligence *per se*, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

NINTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the 49-State Class against Comcast and Citrix)

331. Plaintiff repeats and realleges the preceding factual allegations set forth in paragraphs 1 to 223 as if fully alleged herein.

332. Under the Declaratory Judgments Act, 42 Pa. C.S. § 7531, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief, whether or not further relief is or could be claimed. Furthermore, the Court has broad authority and discretion to restrain acts that are tortious and violate the terms of the laws and regulations described herein.

333. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Comcast and Citrix are each currently maintaining data security measures and cyber-related policies adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Comcast's and Citrix's respective data security measures remain inadequate and Comcast and Citrix remain in possession of Plaintiff's and Class Members' PII and/or provide access to it. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur for as long as Comcast and Citrix each maintain inadequate data security measures.

334. Under its authority pursuant to the Declaratory Judgments Act, this Court should enter a judgment declaring, among other things, the following:

a. Comcast owes a legal duty to secure consumers' PII under the common law, Section 5 of the FTC Act, and the Cable Communications Policy Act;

b. Citrix owes a legal duty to secure consumers' PII under the common law and Section 5 of the FTC Act;

c. Comcast continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII; and

d. Citrix continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII.

335. This Court also should issue corresponding prospective injunctive relief requiring Comcast and Citrix to each employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

336. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Comcast or another entity using Citrix's appliances. The risk of another such breach is real, immediate, and substantial, implicating Plaintiff's direct, substantial, and present interest in the security of his PII. If another breach at Comcast or a similar entity using Citrix's products occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

337. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Comcast or Citrix if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Comcast and Citrix of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Comcast and Citrix each have a pre-existing legal obligation to employ such measures.

338. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Comcast or a similar entity, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully requests that the Court enter judgment in their favor and against Defendants Comcast and Citrix, and prays for relief as follows:

A. For an order certifying the Class under Rules 1702, 1708 and 1709 of the Pennsylvania Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For actual damages, compensatory damages, statutory damages, nominal damages, and statutory penalties, in an amount to be determined, as allowable by law;

D. For punitive damages on behalf of Plaintiff and the Class;

E. For an order of restitution and all other forms of equitable monetary relief, including disgorgement and/or restitution of the revenues wrongfully retained as a result of Comcast's wrongful conduct, as the Court deems appropriate, just, and proper;

F. For declaratory and injunctive relief as described herein, including permanent injunctive relief to prohibit Comcast and Citrix from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

a. Prohibiting Comcast and Citrix from engaging in the wrongful and unlawful acts described herein;

b. Requiring Comcast and Citrix to protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring Comcast to delete, destroy and purge the PII of Plaintiff and Class Members unless Comcast can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring Comcast and Citrix to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. Requiring Comcast and Citrix to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Comcast's and Citrix's respective systems on a periodic basis, and ordering Comcast and Citrix to each promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring Comcast and Citrix to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring Comcast and Citrix to audit, test, and train their security personnel regarding any new or modified procedures;

h. Requiring Comcast to segment data by, among other things, creating firewalls and access controls so that if one area of Comcast's network is

compromised, hackers cannot gain access to other portions of Comcast's systems;

i. Requiring Comcast to conduct regular database scanning and security checks;

j. Requiring Comcast to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

k. Requiring Comcast to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

l. Requiring Comcast to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Comcast's policies, programs and systems for protecting PII;

m. Requiring Comcast to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Comcast's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

n. Requiring Comcast to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

o. Requiring Comcast to implement logging and monitoring programs sufficient to track traffic to and from Comcast servers; and

p. Appointing a qualified and independent third-party assessor to conduct for a period of ten years a SOC 2 Type 2 attestation to evaluate on an annual basis Comcast's and Citrix's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

H. For reimbursement for all other costs and expenses incurred in connection with the prosecution of these claims;

I. For an award of pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: March 25, 2025

Respectfully submitted,

Gary F. Lynch (PA 56887)
Connor P. Hayes (PA 330447)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

Telephone: (412) 322-9243
gary@lcllp.com
connorh@lcllp.com

Charles E. Schaffer (PA 76259)
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
T: (215) 592-1500
cschaffer@lfsblaw.com

James A. Francis (PA 77474)
FRANCIS MAILMAN SOUMILAS, P.C.
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
jfrancis@consumerlawfirm.com

Norman E. Siegel *(pro hac vice forthcoming)*
Stefon J. David *(pro hac vice forthcoming)*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Phone: (816) 714-7100
siegel@stuevesiegel.com
david@stuevesiegel.com

Counsel for Plaintiff and the Proposed Class

VERIFICATION

I, Ryan Emmett, am fully familiar with the facts set forth in this Complaint and hereby certify that the facts set forth in foregoing Complaint are true and correct to the best of my knowledge, or information and belief, and that this statement is made subject to penalties of 18 Pa. C.S.A. § 4904 relating to unsworn falsification to authorities.

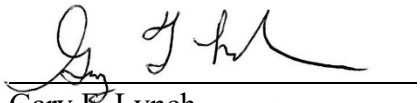
Dated: 3/25/2025

Signed by:
Ryan Emmett
79B2142501694A5...

Ryan Emmett

CERTIFICATE OF COMPLIANCE

I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.



Gary F. Lynch